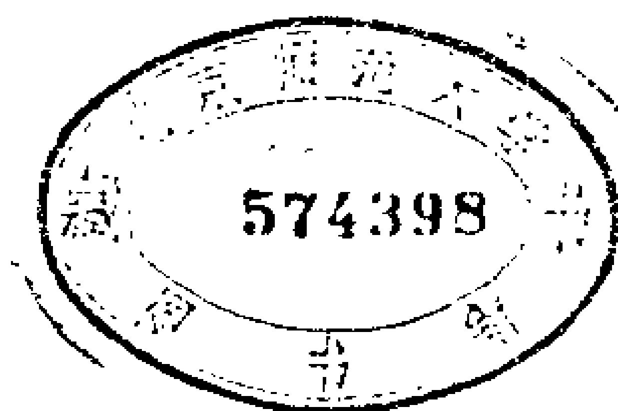
高等学校教学参考书

近世代数基础

(1978年修订本)

张禾瑞著



人民教育出版社

内 容 提 要

本书是张禾瑞同志1952年著《近世代数基础》的修订本。内容除第一版中的基本概念、群论、环与域、整环里的因子分解等四章外，还增加了关于“扩域”的内容。

本书可作为综合大学数学系和高等师范院校有关专业的教学参考书。

高等学校教学参考书

近世代数基础

（1978年修订本）

张禾瑞著

*

人民教育出版社出版

新华书店北京发行所发行

人民教育出版社印刷厂印装

*

1978年5月第1版

1978年9月第1次印刷

书号 13012·0124　　定价0.45元

修订本说明

本书第一版只假定读者有中等数学知识；修订本假定了读者学过我国高等学校的“高等代数”课程．但在修订本的前四章中，除极个别的例子和习题外，并没有用到“高等代数”的知识。所以没有学过高等代数的读者，读前四章还是没有什么困难的．

第一版对于“域”写得较少，所以修订本增加了关于“扩域”的第五章．第一版有加了＊号的“规则的等价关系”和“矩阵环”两节．前者内容比较抽象，有些超出这样一本篇幅小的书的限度；后者内容已见“高等代数”．所以修订本删去了这两节．除此以外，对于原有四章只做了不大的变动，主要是参照中国科学院编订的《数学名词》以及近年来的惯例，改动了某些名词和符号．

修订本的不妥之处，希望读者多提宝贵意见．

我的同事张益敏同志在修订本的抄写和校对方面帮了我的忙，我借此机会表示谢意．

张禾瑞

北京师范大学，一九七八年，三月．

第一版序

（一）本书根据1947—48，1949—50在北京大学教近世代数的材料编成.

（二）本书内容依据中央人民政府教育部1951课改草案，只介绍近世代数的初步理论同基本方法.

（三）本书如用作教本，讲授所需时间也符合上述草案的规定.

（四）我国数学著作多半用文言文. 本书不仅用语体文，并且尽可能用接近口语的语体文. 这是作者的一个尝试. 效果究竟如何，希望读者加以批评.

（五）本书只假定读者有中等数学知识.

（六）作者对于材料的选择，分布与处理，都曾加以特殊的注意. 希望因此可以使初学者对于理论易于了解，对于方法易于掌握，在最短时间内得到阅读近世代数方面较深书籍或文献的能力.

（七）本书差不多在每一章节开始都有一段小引，说明各该章节在全书里的地位. 这些小引能够帮助读者得到对于本书的全面了解.

（八）本书的例同习题都占极重要的地位；读者对于例不可忽略，对于习题越多做越好.

（九）本书第一章是全书的基础，读者必须特别加以注意，细心反复阅读. 这一章的内容虽然比较抽象，由于所包含的实例相当多，据经验一般大学生都能接受.

（十）本书的加＊的正文和习题初学者可以略去.

（十一）本书谈到前面定理，若是只说明定理数目，指的是本节的定理，若是加有其他数目，指的是其他章节的定理．如Ⅱ，3，定理1指的是第二章第三节的定理1．

（十二）本书用符号 $A\Longrightarrow B$ 表明由 A 可以得 B，$A\Longleftrightarrow B$ 表明由 A 可以得 B，由 B 可以得 A．

（十三）本书材料多取自各国在这一方面的标准著作，书名我不在这里一一列举了．

（十四）孙树本教授曾试教本书初稿，魏执权同志在本书的文字方面提了很多宝贵的意见，施惟枢同志在本书的抄写校对方面帮了我很大的忙．我在这里谢谢他们．

张禾瑞

北京大学，一九五二年，一月．

目　录

第一章 基本概念

在普通代数里，我们计算的对象是数，计算的方法是加、减、乘、除．数学渐渐进步，我们发现，可以对于若干不是数的事物，用类似普通计算的方法来加以计算．这种例子我们在高等代数里已经看到很多，例如对于向量、矩阵、线性变换等就都可以进行运算．近世代数（或抽象代数）的主要内容就是研究所谓代数系统，即带有运算的集合．近世代数在数学的其他分支和自然科学的许多部门里都有重要的应用．最近二十多年来，它的一些成果更被直接应用于某些新兴的技术．

我们在高等代数里已初步接触到的群、环、域是三个最基本的代数系统．在本书里我们要对这三个代数系统做略进一步的介绍．

在这一章里，我们先把常要用到的基本概念介绍一下．这些基本概念中的某一些，例如集合和映射，在高等代数里已经出现过，但为了完整起见，我们不得不有所重复．

§1. 集　　合

若干个（有限或无限多个）固定事物的全体叫做一个**集合**（简称**集**）．

组成一个集合的事物叫做这个集合的**元素**（有时简称**元**）．

关于集合，我们常用到几个名词和符号，现在把它们说明一下．

首先我们要规定空集合这一个概念．

定义　一个没有元素的集合叫做**空集合**．

空集合好象没有什么意义，但我们的确有用得到这个概念的

地方．这一点我们不久就会看到．

元素我们一般用小写拉丁字母 $a,b,c,\cdots$ 来表示，集合用大写拉丁字母 $A,B,C,\cdots$ 来表示．一个集合 A 若是由元素 $a,b,c,\cdots$ 作成的，我们用符号

$$A=\{a,b,c,\cdots\}$$

来表示．

若 a 是集合 A 的一个元素，我们说，a 属于 A，或是说，A 包含 a，用符号

$$a\in A \quad 或是 \quad A\ni a$$

来表示．

若 a 不是集合 A 的元素，我们说，a 不属于 A，或是说，A 不包含 a，用符号

$$a\bar{\in} A \quad 或是 \quad A\bar{\ni} a$$

来表示．

定义 若集合 B 的每一个元都属于集合 A，我们说，B 是 A 的**子集**；不然的话，我们说，B 不是 A 的子集．

B 是 A 的子集，我们说，B 属于 A，或是说，A 包含 B，用符号

$$B\subset A \quad 或是 \quad A\supset B$$

来表示．B 不是 A 的子集，我们说，B 不属于 A，或是说，A 不包含 B，用符号

$$B\not\subset A \quad 或是 \quad A\not\supset B$$

来表示．

注意：空集合被认为是任何集合的子集．

定义 若集合 B 是集合 A 的子集，而且至少有一个 A 的元不属于 B，我们就说，B 是 A 的**真子集**；不然的话，我们说，B 不是 A 的真子集．

若集合 A 和集合 B 所包含的元完全一样，那么 A 和 B 表示的

是同一集合，这时我们说，A 等于 B，用符号

$$A=B$$

来表示．显然

$$A=B \Longleftrightarrow A\subset B, B\subset A$$

一个元 a 若同时属于 A 和 B 两个集合，我们说，a 是 A 和 B 的共同元．

定义 集合 A 和集合 B 的所有共同元所组成的集合叫做 A 和 B 的**交集**．

A 和 B 的交集我们用符号

$$A\cap B$$

来表示．

例 1 $A=\{1,2,3\}, B=\{2,5,6\}$．那么

$$A\cap B=\{2\}$$

$A=\{1,2,3\}, B=\{4,5,6\}$．那么

$$A\cap B=\text{空集合}$$

这里，我们看到空集合这个概念的用处．

定义 由至少属于集合 A 和 B 之一的一切元素组成的集合叫做 A 和 B 的**并集**．

A 和 B 的并集我们用符号

$$A\cup B$$

来表示．

例 2 $A=\{1,2,3\}, B=\{2,4,6\}$．那么

$$A\cup B=\{1,2,3,4,6\}$$

$A=\{1,2,3\}, B=\{4,5,6\}$．那么

$$A\cup B=\{1,2,3,4,5,6\}$$

两个以上的集合 A_1，$A_2\cdots$ 的交集、并集的定义和上面完全类似．

定义 令$A_1, A_2, \cdots, A_n$是n个集合．由一切从$A_1, A_2, \cdots, A_n$里顺序取出的元素组$(a_1, a_2, \cdots, a_n)$ $(a_i \in A_i)$所做成的集合叫做**集合$A_1, A_2, \cdots, A_n$的积**，记成

$$A_1 \times A_2 \times \cdots \times A_n$$

习　　题

1．$B \subset A$，但B不是A的真子集，这个情况什么时候才能出现？

2．假定$A \subset B$．$A \cap B = ?$ $A \cup B = ?$

§2．映　　射

在高等代数里已经看到映射这一概念的重要性．现在我们给出这一概念的一个比较一般的定义．

我们看n个集合$A_1, A_2, \cdots, A_n$和另外一个集合D．

定义 假如通过一个法则ϕ，对于任何一个$A_1 \times A_2 \times \cdots \times A_n$的元$(a_1, a_2, \cdots, a_n)(a_i \in A_i)$，都能得到一个唯一的$D$的元$d$，那么这个法则$\phi$叫做集合$A_1 \times A_2 \times \cdots \times A_n$到集合$D$的一个**映射**；元$d$叫做元$(a_1, a_2, \cdots, a_n)$在映射$\phi$之下的**象**；元$(a_1, a_2, \cdots, a_n)$叫做元$d$在$\phi$下的一个**逆象**．

一个映射我们常用以下符号来描写，

$$\phi: \qquad (a_1, a_2, \cdots, a_n) \longrightarrow d = \phi(a_1, a_2, \cdots, a_n)$$

这里，ϕ代表所给的法则，也就是所给的映射；

$$(a_1, a_2, \cdots, a_n) \longrightarrow d$$

表示ϕ替$(a_1, a_2, \cdots, a_n)$这个元规定的象是d；至于$\phi(a_1, a_2, \cdots, a_n)$只是一个符号，就是说，我们有时把$d$这个元写成$\phi(a_1, a_2, \cdots, a_n)$．但这个符号也不是毫无意义的．这个符号暗示，$d$是把$\phi$应用到$(a_1, a_2, \cdots, a_n)$上所得的结果．

在以上的定义中，有几点应该特别加以注意，我们用下面的几

个例来说明一下.

例 1 $A_1=A_2=\cdots=A_n=D=$所有实数作成的集合.

ϕ: $(a_1,a_2,\cdots,a_n)\longrightarrow a_1^2+a_2^2+\cdots+a_n^2=\phi(a_1,a_2,\cdots,a_n)$

是一个$A_1\times A_2\times\cdots\times A_n$到$D$的映射. 这里,$A_i$和$D$都是相同的集合,但这没有什么关系,因为映射的定义并没有说,$A_1,A_2,\cdots,A_n$,D这几个集合中不许有相同的.

例 2 $A_1=\{$东,西$\}$,$A_2=\{$南$\}$,$D=\{$高,低$\}$.

ϕ_1: (西,南)$\longrightarrow$高$=\phi_1$(西,南)

不是一个$A_1\times A_2$到D的映射. 因为,这个ϕ_1只替(西,南)这一个元规定了一个象;但我们从$A_1\times A_2$里还可以取出另一个元来,就是(东,南),替这一个元,ϕ_1并没有规定什么象. 这和定义中一个映射必须替每一个元规定一个象的要求不合.

假如ϕ_2是如下的一个法则

ϕ_2: (西,南)$\longrightarrow$高,(东,南)$\longrightarrow$低

那么ϕ_2是一个$A_1\times A_2$到D的映射.

在例1里,$A_1=A_2=\cdots=A_n$. 对于那里的映射ϕ来说,A_i的次序没有什么关系,比方说,ϕ也是$A_2\times A_1\times\cdots\times A_n$到$D$的映射. 但对例2里的映射$\phi_2$来说,$A_1$和$A_2$的次序不能变动,$\phi_2$不是一个$A_2\times A_1$到$D$的映射. 因为$\phi_2$只替(西,南)和(东,南)各规定了一个象,但并没有替(南,西)和(南,东)规定什么象.

例 3 $A_1=D=$所有实数作成的集合.

ϕ: $a\longrightarrow a$, 若是$a\neq 1$

$1\longrightarrow b$, 这里$b^2=1$

不是一个A_1到D的映射. 因为,这个ϕ固然替每一个不等于1的a规定了一个唯一的象;但通过这个ϕ,我们不能决定b是1还是-1,这就是说,ϕ没有替1规定一个唯一的象. 这是与定义不合的.

例 4　$A_1=D=$所有正整数作成的集合.

$$\phi: \quad a \longrightarrow a-1$$

不是一个 A_1 到 D 的映射. 因为这个 ϕ 固然替每一个 $a\neq 1$ 规定了一个唯一的值 $a-1$; 但当 $a=1$ 的时候, $a-1\overline{\in}D$; 这是与定义不合的.

总括起来说, 我们对于映射的定义应当注意以下几点:

1. 集合 $A_1, A_2, \cdots, A_n, D$ 中可能有几个是相同的;
2. 一般, $A_1, A_2, \cdots, A_n$ 的次序不能掉换;
3. 映射 ϕ 一定要替每一个元 $(a_1, a_2, \cdots, a_n)$ 规定一个象 d;
4. 一个元 $(a_1, a_2, \cdots, a_n)$ 只能有一个唯一的象;
5. 所有的象都必须是 D 的元.

给了集合 $A_1, A_2, \cdots, A_n, D$, 一般来说, 有各种不同的法则可以替每一个元 $(a_1, a_2, \cdots, a_n)$ 规定一个象. 有时两个法则虽然不同, 但它们替每一个元所规定的象却永远相同.

定义　我们说, $A_1\times A_2\times\cdots\times A_n$ 到 D 的两个映射 ϕ_1 和 ϕ_2 是相同的, 假如对于任何一个元 $(a_1, a_2, \cdots, a_n)$ 来说,

$$\phi_1(a_1, a_2, \cdots, a_n)=\phi_2(a_1, a_2, \cdots, a_n)$$

我们所以这样规定的原因是, 两个映射本身是不是相同对于我们并不重要, 重要的是它们的效果是不是相同.

例 5　$A=D=$所有正整数的集合.

$$\phi_1: \quad a \longrightarrow 1=\phi_1(a)$$

$$\phi_2: \quad a \longrightarrow a^0=\phi_2(a)$$

这里替每一个 a 规定象的法则, 换一句话说, 我们的映射, 本身并不相同. 但照我们的定义这两个映射是相同的.

习　题

1. $A=\{1, 2, 3, \cdots, 100\}$. 找一个 $A\times A$ 到 A 的映射.

2. 在你为习题 1 所找到的映射之下，是不是 A 的每一个元都是 $A\times A$ 的一个元的象？

§3. 代数运算

在本章开头已经说过，我们要研究带有运算的集合．现在我们利用映射的概念，来定义代数运算这一个概念．我们看两个集合 A, B 和另一个集合 D.

定义 一个 $A\times B$ 到 D 的映射叫做一个 $A\times B$ 到 D 的**代数运算**.

按照我们的定义，一个代数运算只是一种特殊的映射．在一般映射的定义里，一方面有 n 个集合 $A_1, A_2, \cdots, A_n$ 出现，另一方面有一个集合 D 出现，这里 n 可以是任何正整数．假如我们有一个特殊的映射，它一方面只和两个集合 A, B，另一方面和一个集合 D 发生关系，就把它叫做一个代数运算．让我们看一看，为什么把这样的一个特殊映射叫做代数运算．假定我们有一个 $A\times B$ 到 D 的代数运算．按照定义，给了一个 A 的任意元 a 和一个 B 的任意元 b，就可以通过这个代数运算，得到一个 D 的元 d．我们也可以说，所给代数运算能够对 a 和 b 进行运算，而得到一个结果 d．这正是普通的计算法的特征，比方说，普通加法也不过是能够把任意两个数加起来，而得到另一个数.

代数运算既是一种特殊的映射，描写它的符号，也可以特殊一点．一个代数运算我们用 $\circ$ 来表示，用以前的符号，就可以写

$$\circ: \qquad (a, b) \longrightarrow d = \circ(a, b)$$

我们说过，$\circ(a, b)$ 完全是一个符号，现在为方便起见，不写 $\circ(a, b)$，而写 $a\circ b$．这样，我们描写代数运算的符号，就变成

$$\circ: \qquad (a, b) \longrightarrow d = a\circ b$$

我们举几个例.

例 1　$A=${所有整数}，$B=${所有不等于零的整数}，$D=$ ={所有有理数}.

$$\circ: \quad (a,b)\longrightarrow\frac{a}{b}=a\circ b$$

是一个 $A\times B$ 到 D 的代数运算，也就是普通的除法.

例 2　令 V 是数域 F 上一个向量空间. 那么 F 的数与 V 的向量间的乘法是一个 $F\times V$ 到 V 的代数运算.

例 3　$A=\{1\}, B=\{2\}, D=${奇，偶}.

$$\circ: \quad (1,2)\longrightarrow \text{奇}=1\circ 2$$

是一个 $A\times B$ 到 D 的代数运算.

例 4　$A=\{1,2\}$，$B=\{1,2\}$，$D=${奇，偶}.

$$\circ: \quad (1,1)\longrightarrow\text{奇},\ (2,2)\longrightarrow\text{奇}$$
$$(1,2)\longrightarrow\text{奇},\ (2,1)\longrightarrow\text{偶}$$

是一个 $A\times B$ 到 D 的代数运算.

注意：跟一般映射的情形一样，当 $A=B$ 的时候，A, B 的次序对于一个 $A\times B$ 到 D 的代数运算来说没有什么关系，一个 $A\times B$ 到 D 的代数运算也是一个 $B\times A$ 到 D 的代数运算. 但 A 和 B 的次序可以掉换并不是说，对于 A 的任意元 a，B 的任意元 b，有

$$a\circ b=b\circ a$$

因为 A 和 B 的次序可以掉换只是说，$a\circ b$ 和 $b\circ a$ 都有意义，并不是说，$a\circ b=b\circ a$. 比方说，例 4 的 A, B 就是相等的集合，但

$$1\circ 2=\text{奇}$$
$$2\circ 1=\text{偶}$$

在 A 和 B 都是有限集合的时候，一个 $A\times B$ 到 D 的代数运算，我们常用一个表，叫做运算表来说明. 假定 A 有 n 个元 $a_1, \cdots, a_n$，B 有 m 个元 $b_1, \cdots, b_m$，

$$\circ: \quad (a_i, b_j)\longrightarrow d_{ij}$$

是所给的代数运算. 我们先画一垂线，在这垂线上端画一向右的

横线. 把A的元$a_1, a_2, \cdots, a_n$依次写在垂线的左边，把B的元$b_1, b_2, \cdots, b_m$依次写在横线的上边，然后把对a_i和b_j进行运算后所得结果d_{ij}写在从a_i右行的横线和从b_j下行的垂线的交点上：

	b_1	b_2	$\cdots$	b_m
a_1	d_{11}	d_{12}	$\cdots$	d_{1m}
a_2	d_{21}	d_{22}	$\cdots$	d_{2m}
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	d_{n1}	d_{n2}	$\cdots$	d_{nm}

比方说，例4的代数运算的运算表是

	1	2
1	奇	奇
2	偶	奇

用运算表来说明一个代数运算，常比用箭头或用等式的方法省事，并且清楚.

$A\times B$到D的一般代数运算用到的时候比较少. 最常用的代数运算是$A\times A$到A的代数运算. 在这样的一个代数运算之下，可以对A的任意两个元加以运算，而且所得结果还是在A里面. 所以我们有

定义 假如$\circ$是一个$A\times A$到A的代数运算，我们就说，集合A对于代数运算$\circ$来说是闭的，也说，$\circ$是A的代数运算或**二元运算**.

习 题

1. $A=\{$所有不等于零的偶数$\}$. 找一个集合D，使得普通除法是$A\times A$到D的代数运算. 是不是找得到一个以上的这样的D？

2. $A=\{a, b, c\}$. 规定A的两个不同的代数运算.

§4. 结合律

从上一节的3,4两例，我们可以看出，一个代数运算是可以相当任意规定的，并不一定有多大意义．假如我们任意取几个集合，任意给它们规定几个代数运算，我们很难希望，可以由此算出什么好的结果来．所以以下将遇到的代数运算都适合某些从实际中来的规律．常见的这种规律的第一个，就是结合律．

我们看一个集合 A，一个 $A\times A$ 到 A 的代数运算 $\circ$．

在 A 里任意取出三个元 a,b,c 来，假如我们写下符号

$$a\circ b\circ c$$

那么这个符号没有什么意义，因为代数运算只能对两个元进行运算．但是我们可以先对 a 和 b 进行运算，而得到 $a\circ b$，因为 $\circ$ 是 $A\times A$ 到 A 的代数运算，$a\circ b\in A$，所以我们又可以把这个元同 c 来进行运算，而得到一个结果．这样得来的结果，普通用加括号的方法来表示，所用的步骤也就叫做加括号的步骤．由上面所描写的步骤得来的结果，用加括号的方法写出来，就是

$$(a\circ b)\circ c$$

但我们还有另外一种加括号的步骤，它的结果用加括号的方法写出来是

$$a\circ(b\circ c)$$

在一般情形之下，由这两个不同的步骤所得的结果也未必相同．我们举一个例．

例 $A=\{$所有整数$\}$．代数运算是普通减法．那么

$$(a-b)-c\neq a-(b-c),\quad 除非\ c=0$$

现在我们下一个

定义 我们说，一个集合 A 的代数运算 $\circ$ 适合**结合律**，假如对于 A 的任何三个元 a,b,c 来说，都有

$$(a \circ b) \circ c = a \circ (b \circ c)$$

(注意：a, b, c不一定是不相同的元.)

让我们看一看，结合律有什么作用.

在A里任意取出n个元$a_1, a_2, \cdots, a_n$来，假如我们写下符号

$$a_1 \circ a_2 \circ \cdots \circ a_n$$

这个符号当然也没有意义. 但是假如我们用一个加括号的步骤，当然也会得到一个结果. 加括号的步骤自然不止一种，但因为n是一个有限整数，这种步骤的个数总是一个有限整数. 假定它是N，我们把由这N个步骤所得的结果用

$$\pi_1(a_1 \circ a_2 \circ \cdots \circ a_n), \pi_2(a_1 \circ a_2 \circ \cdots \circ a_n), \cdots, \pi_N(a_1 \circ a_2 \circ \cdots \circ a_n)$$

来表示. 比方说，在上面$n=3$的时候，$N=2$，我们就可以叫

$$\pi_1(a \circ b \circ c) = (a \circ b) \circ c, \pi_2(a \circ b \circ c) = a \circ (b \circ c)$$

这样得来的N个$\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$当然未必相等，但是它们也可能都相等. 我们规定：

定义 假如对于A的n $(n \geqslant 2)$个固定的元$a_1, a_2, \cdots, a_n$来说，所有的$\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$都相等，我们就把由这些步骤可以得到的唯一的结果，用$a_1 \circ a_2 \circ \cdots \circ a_n$来表示.

现在我们证明

定理 假如一个集合A的代数运算$\circ$适合结合律，那么对于A的任意$n (n \geqslant 2)$个元$a_1, a_2, \cdots, a_n$来说，所有的$\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$都相等；因此符号$a_1 \circ a_2 \circ \cdots \circ a_n$也就总有意义.

证明 用数学归纳法.

我们知道，若是只看两个或三个元，定理是对的.

假定，若是元的个数$\leqslant n-1$，定理是对的. 我们说，在这个假定之下，对于一个任意的$\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$来说

$$\pi(a_1 \circ a_2 \circ \cdots \circ a_n) = a_1 \circ (a_2 \circ a_3 \circ \cdots \circ a_n) \tag{1}$$

这一步能够证明，我们的定理也就证明了.

这一个$\pi(a_1\circ a_2\circ\cdots\circ a_n)$是经过一种加括号的步骤所得来的结果，这个步骤的最后一步总是对两个元进行运算：

$$\pi(a_1\circ a_2\circ\cdots\circ a_n)=b_1\circ b_2$$

这里，b_1是前面的若干个，假定是i个元$a_1,a_2,\cdots,a_i$经过一个加括号的步骤所得的结果，b_2是其余的$n-i$个元$a_{i+1},a_{i+2},\cdots,a_n$经过一个加括号的步骤所得的结果．因为$i$和$n-i$都$\leqslant n-1$，由归纳法的假定，

$$b_1=a_1\circ a_2\circ\cdots\circ a_i,\quad b_2=a_{i+1}\circ a_{i+2}\circ\cdots\circ a_n$$

$$\pi(a_1\circ a_2\circ\cdots\circ a_n)=(a_1\circ a_2\circ\cdots\circ a_i)\circ(a_{i+1}\circ a_{i+2}\circ\cdots\circ a_n)$$

假如$i=1$，那么上式就是（1）式，我们用不着再证明什么．假定$i>1$，那么

$$\begin{aligned}\pi(a_1\circ a_2\circ\cdots\circ a_n)&=[a_1\circ(a_2\circ\cdots\circ a_i)]\circ(a_{i+1}\circ a_{i+2}\circ\cdots\circ a_n)\\&=a_1\circ[(a_2\circ\cdots\circ a_i)\circ(a_{i+1}\circ a_{i+2}\circ\cdots\circ a_n)]\\&=a_1\circ(a_2\circ a_3\circ\cdots\circ a_n)\end{aligned}$$

即(1)式仍然成立．证完．

由于这个定理，假如结合律成立，我们就随时都可以应用$a_1\circ a_2\circ\cdots\circ a_n$这个符号，这对于我们当然是一件极方便的事．结合律的重要也就在此．

习　　题

1．$A=\{$所有不等于零的实数$\}$．$\circ$是普通除法：$a\circ b=\frac{a}{b}$．这个代数运算适合不适合结合律？

2．$A=\{$所有实数$\}$．

$\circ$:
$$(a,b)\longrightarrow a+2b=a\circ b$$

这个代数运算适合不适合结合律？

3．$A=\{a,b,c\}$．由表

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

所给的代数运算适合不适合结合律？

§5. 交 换 律

一个代数运算常适合另一个规律，就是交换律.

我们知道，在一个 $A\times A$ 到 D 的代数运算 $\circ$ 之下，$a\circ b$ 未必等于 $b\circ a$. 但是凑巧 $a\circ b$ 也可以等于 $b\circ a$.

定义 我们说，一个 $A\times A$ 到 D 的代数运算 $\circ$ 适合**交换律**，假如对于 A 的任何两个元 a,b 来说，都有

$$a\circ b=b\circ a$$

我们有一个与上节的定理类似的

定理 假如一个集合 A 的代数运算 $\circ$ 同时适合结合律与交换律，那么在 $a_1\circ a_2\circ\cdots\circ a_n$ 里，元的次序可以掉换.

证明 我们用归纳法.

当我们只看一个或两个元的时候，定理是对的.

假定，当元的个数 $=n-1$ 时，定理成立. 在这个假定之下，我们证明，若是把 a_i 的次序任意颠倒一下，而作成一个

$$a_{i_1}\circ a_{i_2}\circ\cdots\circ a_{i_n}$$

这里 $i_1, i_2, \cdots, i_n$ 还是 $1, 2, \cdots, n$ 这 n 个整数，不过次序不同，那么

$$a_{i_1}\circ a_{i_2}\circ\cdots\circ a_{i_n}=a_1\circ a_2\circ\cdots\circ a_n$$

$i_1, i_2, \cdots, i_n$ 中一定有一个等于 n，假定是 i_k. 那么，由于结合律、交换律以及归纳法假定，

$$\begin{aligned}a_{i_1}\circ a_{i_2}\circ\cdots\circ a_{i_n}&=(a_{i_1}\circ\cdots\circ a_{i_{k-1}})\circ[a_n\circ(a_{i_{k+1}}\circ\cdots\circ a_{i_n})]\\&=(a_{i_1}\circ\cdots\circ a_{i_{k-1}})\circ[(a_{i_{k+1}}\circ\cdots\circ a_{i_n})\circ a_n]\end{aligned}$$

$$\overset{\text{结}}{=}[(a_{i_1}\circ\cdots\circ a_{i_{k-1}})\circ(a_{i_{k+1}}\circ\cdots\circ a_{i_n})]\circ a_n$$

$$\overset{\text{归}}{=}(a_1\circ a_2\circ\cdots\circ a_{n-1})\circ a_n$$

$$=a_1\circ a_2\circ\cdots\circ a_n$$

证完

我们普通所习知的重要代数运算，都是适合交换律的. 以后要碰到一些不适合交换律的代数运算. 那时我们会感觉到，计算起来非常不方便. 所以交换律也是一个极重要的规律.

习　　题

1. $A=\{$所有实数$\}$. $\circ$是普通减法：$a\circ b=a-b$. 这个代数运算适合不适合交换律?

2. $A=\{a, b, c, d\}$. 由表

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	d
d	d	c	a	b

所给的代数运算适合不适合交换律?

§6. 分配律

结合律和交换律都只同一种代数运算发生关系. 现在要讨论同两种代数运算发生关系的一种规律，就是分配律. 我们看两种代数运算$\odot$和$\oplus$:

$\odot$ 是一个 $B\times A$ 到 A 的代数运算，

$\oplus$ 是一个 A 的代数运算，

那么，对于任意的 B 的 b 和 A 的 a_1, a_2 来说，

$$b\odot(a_1\oplus a_2)\text{和}(b\odot a_1)\oplus(b\odot a_2)$$

都有意义，都是 A 的元. 但这两个元未必相等.

定义　我们说，代数运算$\odot$，$\oplus$适合第一个分配律，假如对于

B 的任何 b，A 的任何 a_1, a_2 来说，都有

$$b \odot (a_1 \oplus a_2) = (b \odot a_1) \oplus (b \odot a_2)$$

例 假如 B 和 A 都是全体实数的集合，$\odot$ 和 $\oplus$ 就是普通的乘法和加法，那么上式就变成

$$b(a_1 + a_2) = (ba_1) + (ba_2)$$

所以分配律并不是什么奇怪的规则.

现在我们证明

定理 1 假如 $\oplus$ 适合结合律，而且 $\odot$，$\oplus$ 适合第一分配律，那么对于 B 的任何 b，A 的任何 $a_1, a_2, \cdots, a_n$ 来说，

$$b \odot (a_1 \oplus \cdots \oplus a_n) = (b \odot a_1) \oplus \cdots \oplus (b \odot a_n)$$

证明 我们用归纳法. 当 $n=1,2$ 的时候，定理是对的. 假定，当 $a_1, a_2, \cdots$ 的个数只有 $n-1$ 个的时候，定理是对的，现在我们看有 n 个 a_i 时的情形. 这时

$$\begin{aligned} b \odot (a_1 \oplus \cdots \oplus a_n) &= b \odot [(a_1 \oplus \cdots \oplus a_{n-1}) \oplus a_n] \\ &= [b \odot (a_1 \oplus \cdots \oplus a_{n-1})] \oplus (b \odot a_n) \\ &= [(b \odot a_1) \oplus \cdots \oplus (b \odot a_{n-1})] \oplus (b \odot a_n) \\ &= (b \odot a_1) \oplus \cdots \oplus (b \odot a_n) \end{aligned}$$

证完

以上是说的第一个分配律. 第二个分配律同第一个完全类似. 我们看两个代数运算：

$\odot$ 是一个 $A \times B$ 到 A 的代数运算，

$\oplus$ 是一个 A 的代数运算，

那么 $(a_1 \oplus a_2) \odot b$ 和 $(a_1 \odot b) \oplus (a_2 \odot b)$

都有意义.

定义 我们说，代数运算 $\odot$，$\oplus$ 适合第二个分配律，假如，对于 B 的任何 b，A 的任何 a_1, a_2 来说，都有

$$(a_1 \oplus a_2) \odot b = (a_1 \odot b) \oplus (a_2 \odot b)$$

同以上一样，我们有

定理 2 假如$\oplus$适合结合律，而且$\odot$，$\oplus$适合第二分配律，那么对于B的任何b，A的任何$a_1, a_2, \cdots, a_n$来说，

$$(a_1 \oplus \cdots \oplus a_n) \odot b = (a_1 \odot b) \oplus \cdots \oplus (a_n \odot b)$$

分配律的重要性在于它们能叫两种代数运算中有一种联系.

习　题

假定$\odot$，$\oplus$是A的两个代数运算，并且$\oplus$适合结合律，$\odot$，$\oplus$适合两个分配律．证明

$$(a_1 \odot b_1) \oplus (a_1 \odot b_2) \oplus (a_2 \odot b_1) \oplus (a_2 \odot b_2)$$
$$= (a_1 \odot b_1) \oplus (a_2 \odot b_1) \oplus (a_1 \odot b_2) \oplus (a_2 \odot b_2)$$

§7．一一映射、变换

以上讨论了代数运算和代数运算常会满足的几个规律．这些讨论都是普通代数里习见的东西的推广和加深．以下常要把两个集合A和$\bar{A}$加以比较，因此需要进一步研究A到$\bar{A}$的映射.

先看两个例子.

例 1　$A = \{1, 2, 3, 4, 5\}$，$\bar{A} = \{2, 4, 6, 8\}$．那么

ϕ:　　$1 \longrightarrow 2$，$2 \longrightarrow 4$，$3 \longrightarrow 6$，$4 \longrightarrow 2$，$5 \longrightarrow 2$

是一个A到$\bar{A}$的映射.

例 2　$A = \{1, 2, 3, \cdots\}$，$\bar{A} = \{$奇，偶$\}$．那么

ϕ:　　$1, 3, 5, \cdots \longrightarrow$ 奇；$2, 4, 6, \cdots \longrightarrow$ 偶

是一个A到$\bar{A}$的映射.

在例 1 里，$\bar{A}$的元 8 不是A的任何元的象，而在例 2 里，$\bar{A}$的两个元却都是A中某些元的象.

定义　若是在一个集合A到集合$\bar{A}$的映射ϕ下，$\bar{A}$的每一个元都至少是A中某一个元的象，那么ϕ叫做一个A到$\bar{A}$的**满射**.

一般，在一个A到$\bar{A}$的映射之下，A里的若干个不同的元在$\bar{A}$里有一个相同的象，比方说在例 2 里，A的不同的元 1，3，…在$\bar{A}$

里的象都是奇，A 的不同的元 $2,4,\cdots$ 在 $\bar{A}$ 里的象都是偶.

但在一个 A 到 $\bar{A}$ 的映射之下，可能 A 里的不同的元在 $\bar{A}$ 里的象也不相同.

定义 一个 A 到 $\bar{A}$ 的映射

$$\phi: \qquad a \longrightarrow \bar{a}$$

叫做一个 A 到 $\bar{A}$ 的**单射**，假如

$$a \neq b \Longrightarrow \bar{a} \neq \bar{b}$$

一个既是满射又是单射的映射特别重要.

定义 假如一个集合 A 到集合 $\bar{A}$ 的映射 ϕ 既是满射又是单射，那么 ϕ 叫做一个 A 与 $\bar{A}$ 间的**一一映射**.

在一个 A 与 $\bar{A}$ 间的一一映射之下，$\bar{A}$ 的每一个元都是而且只是 A 里面一个元的象. 我们举一个例.

例 3 $A=\{1,2,3,\cdots\}$，$\bar{A}=\{2,4,6,\cdots\}$. 那么，

$$\phi: \qquad 1 \longrightarrow 2,\ 2 \longrightarrow 4, \cdots$$

是一个 A 与 $\bar{A}$ 间的一一映射.

一一映射有以下的重要性质：

定理 一个 A 与 $\bar{A}$ 间的一一映射 ϕ 带来一个通常用 ϕ^{-1} 表示的 $\bar{A}$ 与 A 间的一一映射.

证明 首先我们利用 ϕ 来作一个 $\bar{A}$ 到 A 的映射 ϕ^{-1}，这就是说，我们利用 ϕ 来替 $\bar{A}$ 的每一个元 $\bar{a}$ 规定一个唯一的在 A 里面的象. 我们规定，

$$\phi^{-1}: \qquad \bar{a} \longrightarrow a = \phi^{-1}(\bar{a}), \text{假如 } \bar{a} = \phi(a)$$

由于 ϕ 是 A 与 $\bar{A}$ 间的一一映射，给了 $\bar{A}$ 的一个任意的 $\bar{a}$，有而且只有一个 A 的 a 能够满足条件 $\phi(a)=\bar{a}$，这就是说，给了 $\bar{A}$ 的一个任意的 $\bar{a}$，由于规则 ϕ^{-1}，我们能而且只能得到一个 A 的 a. 这样，ϕ^{-1} 是一个 $\bar{A}$ 到 A 的映射.

现在我们证明 ϕ^{-1} 是 $\bar{A}$ 与 A 间的一一映射.

(i) ϕ^{-1} 是 $\bar{A}$ 到 A 的满射，换一句话说，在 ϕ^{-1} 之下，A 的每一元 a 都是 $\bar{A}$ 的某一元的象．因为，给了 A 的一个任意元 a，一定有一个 $\bar{A}$ 的元 $\bar{a}$，满足条件 $\bar{a}=\phi(a)$．这样，

ϕ^{-1}:　　　　　　这个 $\bar{a}\longrightarrow$给的 a

(ii)　　　　　　$\bar{a}\neq\bar{b}\Longrightarrow\phi^{-1}(\bar{a})\neq\phi^{-1}(\bar{b})$

因为，由 ϕ^{-1} 的定义，

ϕ:　　　　　　$\phi^{-1}(\bar{a})\longrightarrow\bar{a}$

　　　　　　　　$\phi^{-1}(\bar{b})\longrightarrow\bar{b}$

若是 $\phi^{-1}(\bar{a})=\phi^{-1}(\bar{b})$，那么 $\bar{a}$ 和 $\bar{b}$ 是同一个元在 ϕ 之下的象，因而 $\bar{a}=\bar{b}$，与假定冲突．证完．□

这样 ϕ 和 ϕ^{-1} 正象作用力和反作用力一样，永远同时存在．因此，一个 A 与 $\bar{A}$ 间的一一映射 ϕ 我们也常用符号

ϕ:　　　　　　$a\longleftrightarrow\bar{a}$

来表示．这里，向右的箭头表示 ϕ 的作用，向左的箭头却表示 ϕ^{-1} 的作用，不过我们没有把 ϕ^{-1} 明写出来罢了．由于同一理由，对于一个一一映射 ϕ 来说，A 与 $\bar{A}$ 的次序所占的地位不太重要，因此，我们把 ϕ 叫做 A 与 $\bar{A}$ 间的一一映射．

注意：假如 A 与 $\bar{A}$ 间有一个一一映射存在，而 A 是有限集合，那么显然 $\bar{A}$ 也是有限集合，而且 A 与 $\bar{A}$ 所包含的元一样多，因此，一个有限集合与它的一个真子集间不能有一一映射存在．但当 A 与 $\bar{A}$ 是无限集合的时候，情形完全不同，上面例 3 里的 A 与 $\bar{A}$ 间有一个一一映射存在，可是 $\bar{A}$ 的确是 A 的真子集．

结尾我们还要规定几个名词．在一个映射里出现的 A 和 $\bar{A}$ 当然可以是相同的集合．

定义　一个 A 到 A 的映射叫做 A 的一个**变换**．

一个 A 到 A 的满射、单射或 A 与 A 间的一一映射叫做 A 的一个**满射变换、单射变换或一一变换**．

变换，尤其是一一变换，也是近世代数里极重要的概念。

例 4　$A=\{$所有实数$\}$.

τ:
$$x \longrightarrow e^x$$
是 A 的一个单射变换.

例 5　$A=\{$所有整数$\}$.

τ:
$$a \longrightarrow \frac{a}{2}, \qquad \text{假如 } a \text{ 是偶数}$$
$$a \longrightarrow \frac{a+1}{2}, \qquad \text{假如 } a \text{ 是奇数}$$
是 A 的一个满射变换.

例 6　$A=\{1,2,3\}$.

τ_1:　$1 \longrightarrow 1,\ 2 \longrightarrow 2,\ 3 \longrightarrow 3$

τ_2:　$1 \longrightarrow 2,\ 2 \longrightarrow 3,\ 3 \longrightarrow 1$

都是 A 的一一变换.

习　题

1. $A=\{$所有>0的实数$\}$，$\bar{A}=\{$所有实数$\}$. 找一个 A 与 $\bar{A}$ 间的一一映射.

2. $A=\{$所有$\geqslant 0$的实数$\}$，$\bar{A}=\{$所有实数 $\bar{a}$，$0 \leqslant \bar{a} \leqslant 1\}$. 找一个 A 到 $\bar{A}$ 的满射.

3. 假定 ϕ 是 A 与 $\bar{A}$ 间的一个一一映射，a 是 A 的一个元.
$$\phi^{-1}[\phi(a)]=?\quad \phi[\phi^{-1}(a)]=?$$
若 ϕ 是 A 的一个一一变换，这两个问题的回答又该是什么？

§8. 同　态

上一节所说的映射，只与两个集合 A 和 $\bar{A}$ 发生关系. 但我们以后很少单独地考察集合，而是要看有代数运算的集合. 因此，在这一节里我们要讨论到也与代数运算发生关系的映射. 这是近世代数里一等重要的概念.

我们看两个集合 A 和 $\bar{A}$. 假定有一个 A 的代数运算$\circ$，一个 $\bar{A}$ 的代数运算$\bar{\circ}$，并且有一个 A 到 $\bar{A}$ 的映射 ϕ.

假如 a 和 b 是 A 的两个元，那么 $\phi(a\circ b)$，和 $\phi(a)\bar{\circ}\phi(b)$ 都有意义，都是 $\bar{A}$ 的元. 现在我们问，是否

$$\phi(a\circ b)=\phi(a)\bar{\circ}\phi(b) \tag{1}$$

换一句话说，假定在 ϕ 之下，

$$a\longrightarrow\bar{a},\quad b\longrightarrow\bar{b}$$

我们问，是否在 ϕ 之下，

$$a\circ b\longrightarrow\bar{a}\bar{\circ}\bar{b} \tag{2}$$

由下面的例 3，我们将要看到，(1)，(2) 一般不能成立. 这并没有什么希奇，因为 ϕ 根本同$\circ$，$\bar{\circ}$ 这两个代数运算没有什么关系，ϕ 替 $a\circ b$ 规定的象，未必就刚好是 $\bar{a}\bar{\circ}\bar{b}$. 现在我们下一个

定义 一个 A 到 $\bar{A}$ 的映射 ϕ，叫做一个对于代数运算$\circ$和$\bar{\circ}$来说的，A 到 $\bar{A}$ 的[illegible]，假如，在 ϕ 之下，不管 a 和 b 是 A 的哪两个元，只要

$$a\longrightarrow\bar{a},\quad b\longrightarrow\bar{b}$$

就有

$$a\circ b\longrightarrow\bar{a}\bar{\circ}\bar{b}$$

我们举几个例. 看以下的集合和代数运算：

$A=\{$所有整数$\}$，A 的代数运算是普通加法.

$\bar{A}=\{1,-1\}$，$\bar{A}$ 的代数运算是普通乘法.

例 1 ϕ_1: $\qquad a\longrightarrow 1 \qquad$ (a 是 A 的任一元)

是一个 A 到 $\bar{A}$ 的同态映射. ϕ_1 是一个 A 到 $\bar{A}$ 的映射，显然. 对于 A 的任意两个整数 a 和 b 来说，我们有

$$a\longrightarrow 1,\quad b\longrightarrow 1$$

$$a+b\longrightarrow 1=1\times 1$$

例 2 ϕ_2: $\qquad a\longrightarrow 1, \qquad$ 若 a 是偶数

$\qquad\qquad\qquad a\longrightarrow -1, \qquad$ 若 a 是奇数

ϕ_2是一个A到$\bar{A}$的满射的同态映射. ϕ_2是A到$\bar{A}$的满射，显然. 对于A的任意两个整数a和b来说:

若a, b都是偶数,那么

$$a \longrightarrow 1,\quad b \longrightarrow 1$$

$$a+b \longrightarrow 1 = 1 \times 1$$

若a, b都是奇数,那么

$$a \longrightarrow -1,\quad b \longrightarrow -1$$

$$a+b \longrightarrow 1 = (-1) \times (-1)$$

若a奇，b偶,那么

$$a \longrightarrow -1,\quad b \longrightarrow +1$$

$$a+b \longrightarrow -1 = (-1) \times (+1)$$

a偶,b奇时,情形一样.

例3 ϕ_3: $a \longrightarrow -1$ （a是A的任一元）

固然是一个A到$\bar{A}$的映射,但不是同态映射. 因为,对于任意A的a和b来说,

$$a \longrightarrow -1,\quad b \longrightarrow -1$$

$$a+b \longrightarrow -1 \neq (-1) \times (-1)$$

A到$\bar{A}$的满射的同态映射对于我们比较重要. 关于这种同态映射,我们还要规定一个术语.

定义 假如对于代数运算$\circ$和$\bar{\circ}$来说,有一个A到$\bar{A}$的满射的同态映射存在,我们就说,这个映射是一个**同态满射**,并说,对于代数运算$\circ$和$\bar{\circ}$来说,A与$\bar{A}$同态.

同态满射的最大用处在比较两个集合. 现在我们证明几个定理,来看一看同态满射在比较两个集合时的效果.

定理1 假定,对于代数运算$\circ$和$\bar{\circ}$来说,A与$\bar{A}$同态. 那么,(i)若$\circ$适合结合律,$\bar{\circ}$也适合结合律;(ii)若$\circ$适合交换律,$\bar{\circ}$也适合交换律.

证明 我们用 ϕ 来表示 A 到 $\bar{A}$ 的同态满射.

(i) 假定 $\bar{a}$, $\bar{b}$, $\bar{c}$ 是 $\bar{A}$ 的任意三个元. 那么，我们在 A 里至少找得出三个元 a, b, c 来，使得在 ϕ 之下，

$$a \longrightarrow \bar{a}, \quad b \longrightarrow \bar{b}, \quad c \longrightarrow \bar{c}$$

于是，由于 ϕ 是同态满射，

$$a \circ (b \circ c) \longrightarrow \bar{a} \bar{\circ} (\overline{b \circ c}) = \bar{a} \bar{\circ} (\bar{b} \bar{\circ} \bar{c})$$

$$(a \circ b) \circ c \longrightarrow (\overline{a \circ b}) \bar{\circ} \bar{c} = (\bar{a} \bar{\circ} \bar{b}) \bar{\circ} \bar{c}$$

但由题设，
$$a \circ (b \circ c) = (a \circ b) \circ c$$

这样，$(\bar{a} \bar{\circ} \bar{b}) \bar{\circ} \bar{c}$ 和 $\bar{a} \bar{\circ} (\bar{b} \bar{\circ} \bar{c})$ 是 A 里同一元的象，因而
映射之义
$$\bar{a} \bar{\circ} (\bar{b} \bar{\circ} \bar{c}) = (\bar{a} \bar{\circ} \bar{b}) \bar{\circ} \bar{c}$$

(ii) 我们看 $\bar{A}$ 的任意两个元 $\bar{a}, \bar{b}$，并且假定，在 ϕ 之下，

$$a \longrightarrow \bar{a}, \quad b \longrightarrow \bar{b} \qquad (a, b \in A)$$

那么
$$a \circ b \longrightarrow \overline{a \circ b}, \quad b \circ a \longrightarrow \overline{b \circ a}$$

但
$$a \circ b = b \circ a$$

所以
$$\bar{a} \bar{\circ} \bar{b} = \bar{b} \bar{\circ} \bar{a}$$
证完

定理 2 假定，$\odot$, $\oplus$ 都是集合 A 的代数运算，$\bar{\odot}$, $\bar{\oplus}$ 都是集合 $\bar{A}$ 的代数运算，并且存在一个 A 到 $\bar{A}$ 的满射 ϕ，使得 A 与 $\bar{A}$ 对于代数运算 $\odot$, $\bar{\odot}$ 来说同态，对于代数运算 $\oplus$, $\bar{\oplus}$ 来说也同态. 那么，(i) 若 $\odot$, $\oplus$ 适合第一分配律，$\bar{\odot}$, $\bar{\oplus}$ 也适合第一分配律；(ii) 若 $\odot$, $\oplus$ 适合第二分配律，$\bar{\odot}$, $\bar{\oplus}$ 也适合第二分配律.

证明 我们只证明 (i)，(ii) 可以完全类似地证明.

看 $\bar{A}$ 的任意三个元 $\bar{a}, \bar{b}, \bar{c}$，并且假定

$$a \longrightarrow \bar{a}, \quad b \longrightarrow \bar{b}, \quad c \longrightarrow \bar{c} \qquad (a, b, c \in A)$$

那么
$$a \odot (b \oplus c) \longrightarrow \bar{a} \bar{\odot} (\overline{b \oplus c}) = \bar{a} \bar{\odot} (\bar{b} \bar{\oplus} \bar{c})$$

$$(a \odot b) \oplus (a \odot c) \longrightarrow (\overline{a \odot b}) \bar{\oplus} (\overline{a \odot c}) = (\bar{a} \bar{\odot} \bar{b}) \bar{\oplus} (\bar{a} \bar{\odot} \bar{c})$$

但
$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

所以 满射
$$\bar{a} \bar{\odot} (\bar{b} \bar{\oplus} \bar{c}) = (\bar{a} \bar{\odot} \bar{b}) \bar{\oplus} (\bar{a} \bar{\odot} \bar{c})$$
证完

习　题

1. $A=\{$所有实数 $x\}$，A 的代数运算是普通乘法．以下映射是不是 A 到 A 的一个子集 $\bar{A}$ 的同态满射？

a) $x\to|x|$　b) $x\to 2x$　c) $x\to x^2$　d) $x\to -x$

2. 假定 A 和 $\bar{A}$ 对于代数运算 $\circ$ 和 $\bar{\circ}$ 来说同态，$\bar{A}$ 和 $\bar{\bar{A}}$ 对于代数运算 $\bar{\circ}$ 和 $\bar{\bar{\circ}}$ 来说同态．证明，A 和 $\bar{\bar{A}}$ 对于代数运算 $\circ$ 和 $\bar{\bar{\circ}}$ 来说同态．

§9．同构、自同构

一同态满射一般不是一个一一映射，它在比较两个集合时的效果，在上一节已看到．但一同态满射可能同时是一个一一映射．这种加强的同态映射在比较集合时更有效，对我们也更重要．

定义　我们说，一个 A 与 $\bar{A}$ 间的一一映射 ϕ 是一个对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说的，A 与 $\bar{A}$ 间的同构映射（简称同构），假如在 ϕ 之下，不管 a,b 是 A 的哪两个元，只要

$$a\longrightarrow\bar{a},\quad b\longrightarrow\bar{b}$$

就有

$$a\circ b\longrightarrow\bar{a}\,\bar{\circ}\,\bar{b}$$

假如在 A 与 $\bar{A}$ 间，对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说，存在一个同构映射，我们说，对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说，A 与 $\bar{A}$ 同构，并且用符号

$$A\cong\bar{A}$$

来表示．

例 1　$A=\{1,2,3\}$，$\bar{A}=\{4,5,6\}$．

	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

	4	5	6
4	6	6	6
5	6	6	6
6	6	6	6

各是 A 与 $\bar{A}$ 的代数运算 $\circ$ 与 $\bar{\circ}$ 的表. 那么

$$1 \longrightarrow 4,\ 2 \longrightarrow 5,\ 3 \longrightarrow 6$$

是一个 A 与 $\bar{A}$ 间的同构映射. 因为:

$$a \circ b = 3 \longrightarrow 6 = \bar{a} \bar{\circ} \bar{b}$$

我们要注意,假如 ϕ 是 A 与 $\bar{A}$ 间的同构映射,那么 ϕ^{-1} 也是 $\bar{A}$ 与 A 间的同构映射. 因为,在 ϕ^{-1} 之下,只要

$$\bar{a} \longrightarrow a,\ \bar{b} \longrightarrow b$$

显然就有

$$\bar{a} \bar{\circ} \bar{b} \longrightarrow a \circ b$$

所以同构映射与 A 和 $\bar{A}$ 的次序没有多大关系.

现在我们要看一看,同构映射在比较集合时的效果.

我们先来研究一下例 1. 在这个例里, A 有三个元, 是 1,2,3. $\bar{A}$ 也有三个元,是 4,5,6. 我们问, A 和 $\bar{A}$ 有没有什么区别? 当然有. 因为 1,2,3 和 4,5,6 是不相同的东西. 但是, 我们所以说 1,2,3 和 4,5,6 不同, 是因为我们知道, 它们都是普通整数, 整数 1, 2,3 和整数 4,5,6 当然有区别. 现在让我们来看一看 A 的代数运算 $\circ$. 应用这个运算于 1 和 1 得 3, 于 1 和 2 也得 3, 于 3 和 2 得 3, 于 3 和 3 还是得 3. 我们问,我们习见的普通整数 1,2,3,是否适合过这种规律? 回答是,从来没有. 这就是说,对于 A 的代数运算 $\circ$ 来说, A 的元 1, 2, 3 早已失去了普通整数 1, 2, 3 的意义. 同样,对于 $\bar{A}$ 的代数运算 $\bar{\circ}$ 来说, $\bar{A}$ 的元 4,5,6 也早已失去了普通整数 4,5,6 的意义. 这样, 我们方才是把已经失去了整数意义的东西仍旧看作了整数, 而由此就断定了这些东西是不相同的. 可以说, 我们的结论下得太快了一点. 现在我们不把 A 的 1,2,3 和 $\bar{A}$ 的 4,5,6 看成普通整数,再来作一个比较. 那么 A 有三个元,第一个叫做 1, 第二个叫做 2,第三个叫做 3. A 有一个代数运算,叫做 $\circ$. 应用这个运算于 A 的任意两个元所得结果总是第三个元.

$\bar{A}$ 也有三个元，第一个叫做 4，第二个叫做 5，第三个叫做 6．$\bar{A}$ 也有一个代数运算，叫做 $\bar{\circ}$．应用这个运算于 $\bar{A}$ 的任意两个元所得结果也总是第三个元．这样看起来，A 同 $\bar{A}$ 实在没有什么本质上的区别．唯一的区别只是命名的不同而已．

现在我们看两个任意的，对于代数运算 $\circ$ 和 $\bar{\circ}$ 来说是同构的集合 A 和 $\bar{A}$．我们可以假定，

$$A=\{a, b, c, \cdots\}$$
$$\bar{A}=\{\bar{a}, \bar{b}, \bar{c}, \cdots\}$$

并且在 A 与 $\bar{A}$ 间的同构映射 ϕ 之下，

$$a \longleftrightarrow \bar{a}, \quad b \longleftrightarrow \bar{b}, \quad c \longleftrightarrow \bar{c}, \cdots$$

由于同构映射的性质，我们知道，

$$x \circ y=z \Longleftrightarrow \bar{x} \bar{\circ} \bar{y}=\bar{z}$$

这就是说，代数运算 $\circ$ 在 A 里规定的运算规则同代数运算 $\bar{\circ}$ 在 $\bar{A}$ 里规定的运算规则完全类似，唯一的不同就在一方面有小横而另一方面没有．因此，A 如果有一个性质，这个性质是完全可以用代数运算 $\circ$ 计算得来的，那么 $\bar{A}$ 就有一个完全类似的性质．反过来说，$\bar{A}$ 的一个只同代数运算 $\bar{\circ}$ 有关的性质也决定一个完全类似的 A 的性质（参看 I，8 定理 1，2）．这就是说，若是仅就代数运算 $\circ$ 对 A，代数运算 $\bar{\circ}$ 对 $\bar{A}$ 所发生的影响来看，A 与 $\bar{A}$ 只有形式上的不同，而没有什么本质上的区别．当然 A 与 $\bar{A}$ 的元一般是不相同的东西；但正如我们在本节开头所讨论的情形一样，这种不同是受外来的影响而产生的．

总括起来我们得到结论：

假定对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说，A 与 $\bar{A}$ 同构．那么，对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说，A 与 $\bar{A}$ 这两个集合，抽象地来看，没有什么区别（只有命名上的不同）．若一个集合有一个只与这个集合的代数运算有关的性质，那么另一个集合有一个完全类似的性质．

这样，同构映射是比较两个集合时最有效的工具。

最后我们还要规定一个名词．一个集合 A 同 A 自己之间当然也可以有同构映射存在．假定 $\circ$ 是一个 A 的代数运算．

定义 对于 $\circ$ 与 $\circ$ 来说的一个 A 与 A 间的同构映射叫做一个对于 $\circ$ 来说的 A 的**自同构**．

自同构映射也是一个极重要的概念．

例 2 $A=\{1,2,3\}$．代数运算 $\circ$ 由下表给定：

	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

那么

$$\phi: \quad 1 \longrightarrow 2, \quad 2 \longrightarrow 1, \quad 3 \longrightarrow 3$$

是一个对于 $\circ$ 来说的 A 的自同构．

习 题

1．$A=\{a,b,c\}$．代数运算 $\circ$ 由下表给定

	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

找出所有 A 的一一变换．对于代数运算 $\circ$ 来说，这些一一变换是否都是 A 的自同构？

2．$A=\{$所有有理数$\}$．找一个 A 的对于普通加法来说的自同构（映射 $x\leftrightarrow x$ 除外）．

3.* $A=\{$所有有理数$\}$；A 的代数运算是普通加法．$\bar{A}=\{$所有 $\neq 0$ 的有理数$\}$；$\bar{A}$ 的代数运算是普通乘法．证明，对于给的代数运算来说，A 与 $\bar{A}$ 间没有同构映射存在（先决定 0 在一个同构映射之下的象）．

§10. 等价关系与集合的分类

我们将来除了把两个集合拿来比较之外，有时也要把一个集合分成若干个子集来加以讨论. 这时就要用到集合的分类这一个概念. 这个概念和另外一个叫做等价关系的基本概念有密切的关系. 在这一节里，我们要讨论一下这两种概念.

我们先规定什么叫做关系.

我们看一个集合 A 同另一个集合 D，D 只包含两个元，就是"对"和"错"这两个字.

定义 一个 $A\times A$ 到 D 的映射 R 叫做 A 的元间的一个关系. 若 $R(a,b)=$ 对，我们说，a 与 b 符合关系 R，记成 aRb. 若 $R(a,b)=$ 错，我们说，a 与 b 不符合关系 R.

由这个定义，给了 A 的元间的一个关系，我们可以决定，任意一对 A 的元 a,b 是否符合这个关系.

例 1 $A=\{$所有实数$\}$.

R: $(a,b)\longrightarrow$ 对，若是 $b-a$ 是正的

$(a,b)\longrightarrow$ 错，若是 $b-a$ 不是正的

是 A 的元间的一个关系. 这也就是我们普通用符号 $<$ 表示的关系.

等价关系是一种特殊的关系，占的地位特别重要，这种关系我们一般用 $\sim$ 来表示.

定义 集合 A 的元间的一个关系 $\sim$ 叫做一个等价关系，假如 $\sim$ 满足以下规律:

Ⅰ. **反射律**: $a\sim a$，不管 a 是 A 的哪一个元

Ⅱ. **对称律**: $a\sim b\Longrightarrow b\sim a$

Ⅲ. **推移律**: $a\sim b,\ b\sim c\Longrightarrow a\sim c$

若 $a\sim b$，我们说，a 与 b 等价.

我们举一个例.

例 2　“等于”这个关系是一个等价关系.

现在我们规定什么叫做集合的分类.

定义　若把一个集合 A 分成若干个叫做类的子集，使得 A 的每一个元属于而且只属于一个类，那么这些类的全体叫做**集合 A 的一个分类**.

等价关系与集合的分类的关系由以下两个定理可以看出.

定理 1　集合 A 的一个分类决定 A 的元间的一个等价关系.

证明　我们利用给的分类来作一个等价关系. 我们规定，

$$a \sim b,\ \text{当而且只当 } a, b \text{ 同在一类的时候}$$

这样规定的 $\sim$ 显然是 A 的元间的一个关系. 我们证明，它是一个等价关系.

Ⅰ. a 与 a 同在一类，所以 $a \sim a$.

Ⅱ. 若是 a 与 b 同在一类，那么 b 与 a 也同在一类，所以

$$a \sim b \Longrightarrow b \sim a$$

Ⅲ. 若是 a, b 同在一类，b, c 同在一类，那么 a, c 也同在一类，所以

$$a \sim b,\ b \sim c \Longrightarrow a \sim c$$

证完

定理 2　集合 A 的元间的一个等价关系 $\sim$ 决定 A 的一个分类.

证明　我们利用给定的等价关系来作一个 A 的分类. 把所有同 A 的一个固定的元 a 等价的元都放在一起，作成一个子集，这个子集用符号 $[a]$ 来表示. 我们说，所有这样得到的子集就作成 A 的一个分类. 我们分三步来证明这一点.

(i)
$$a \sim b \Longrightarrow [a] = [b]$$

假定
$$a \sim b$$

那么，由等价关系的性质Ⅲ以及 $[a]$ 和 $[b]$ 的定义，

$$c \in [a] \Longrightarrow c \sim a \Longrightarrow c \sim b \Longrightarrow c \in [b]$$

这就是说，

(1) $$[a]\subset[b]$$

但由等价关系的性质Ⅱ,

$$b\sim a$$

因此同样可推得

(2) $$[b]\subset[a]$$

由(1)与(2), $$[a]=[b]$$

(ii) A的每一个元a只能属于一个类.

假定 $$a\in[b],\quad a\in[c]$$

那么由$[b]$,$[c]$的定义,

$$a\sim b,\ a\sim c$$

这样,由Ⅱ,Ⅲ, $$b\sim c$$

于是由(i), $$[b]=[c]$$

(iii) A的每一个元a的确属于某一个类.

因为,由Ⅰ以及上述类的定义,

$$a\in[a]$$

证完

关于集合的分类我们常要用到以下的两个名词.

定义 假定我们有一个集合的一个分类. 那么,一个类里的任何一个元叫做这个类的一个代表. 刚好由每一类的一个代表作成的集合叫做一个全体代表团.

我们再举一个例.

例3 $A=\{\cdots,-2,-1,0,1,2,\cdots\}$.

我们取一个固定的整数$n>0$, 利用这个n, 我们规定A的元间的一个关系R,

$$aRb,\ \text{当而且只当}\ n\mid a-b\ \text{的时候}$$

这里, 符号$n\mid a-b$表示n能整除$a-b$. 这显然是一个等价关系. 这个等价关系普通叫做模n的同余关系, 并且用

$$a\equiv b\quad(n)$$

来表示(读成 a 同余 b 模 n).

这个等价关系决定 A 的一个分类. 这样得来的类叫做模 n 的**剩余类**. 让我们看一看，这些个剩余类是什么样子. 我们容易看出，任意一个整数一定与 $0,1,\cdots,n-1$ 这 n 个整数中的一个同余；另一方面，$0,1,\cdots,n-1$ 这 n 个整数中的任意两个不同的整数都不同余. 因此我们刚好有 n 个不同的剩余类，就是：

$$[0]=\{\cdots,\quad -2n,\quad -n,\quad 0,\quad n,\quad 2n,\cdots\}$$

$$[1]=\{\cdots,-2n+1,-n+1,\quad 1,\quad n+1,2n+1,\cdots\}$$

……………………………………………………

$$[n-1]=\{\cdots,\quad -n-1,\quad -1,n-1,2n-1,3n-1,\cdots\}$$

我们通常用 $0,1,\cdots,n-1$ 来作这 n 个类的全体代表团. 当然也可以用另外的 n 个数，比方说 $1,2,\cdots,n$.

注意：我们只是为说明方便起见，在上面假定 $n>0$. 实际上，当 n 是 <0 的整数的时候，可以完全同样地规定模 n 的同余关系. 由此得到的剩余类与模 $|n|$ 的剩余类完全一样.

习　题

1. $A=\{$所有实数$\}$. A 的元间的关系 $>$ 以及 $\geqslant$ 是不是等价关系？

2.* 有人说：假如一个关系 R 适合对称律和推移律，那么它也适合反射律. 他的推论方法是：因为 R 适合对称律，

$$aRb \Longrightarrow bRa$$

因为 R 适合推移律，

$$aRb,\ bRa \Longrightarrow aRa$$

这个推论方法有什么错误？

3. 仿照例 3 规定整数间的关系

$$a\equiv b\quad(-5)$$

证明你所规定的是一个等价关系，并且找出模 -5 的剩余类.

第二章　群　论

有了前一章的准备工作以后，我们现在来讨论群这个代数系统.

群只有一种代数运算. 我们已经看到，一个代数运算用什么符号来表示，是可以由我们自由决定的，有时可以用 $\circ$，有时可以用 $\bar{\circ}$. 一个群的代数运算普通为便利起见，不用 $\circ$ 来表示，而用普通乘法的符号来表示，就是我们不写 $a \circ b$，而写 ab. 并且因此我们就把一个群的代数运算叫做乘法. 当然一个群的乘法一般不是普通的乘法. 现在我们要看一看，什么叫群.

§1. 群的定义

群的定义比较常见的有两种. 我们先看第一种.

群的第一定义　我们说，一个不空集合 G 对于一个叫做乘法的代数运算来说作成一个群，假如

Ⅰ. G 对于这个乘法来说是闭的；

Ⅱ. 结合律成立：

$$a(bc)=(ab)c$$

对于 G 的任意三个元 a, b, c 都对；

Ⅲ. 对于 G 的任意两个元 a, b 来说，方程

$$ax=b \quad 和 \quad ya=b$$

都在 G 里有解.

例1　G 只包含一个元 g. 乘法是 $gg=g$. G 对于这个乘法来说作成一个群. 因为

Ⅰ. G 是闭的;

Ⅱ. $g(gg)=(gg)g=g$;

Ⅲ. $gx=g$ 有解,就是 g,

$yg=g$ 有解,就是 g.

例 2 G 是全体整数的集合. G 对于普通加法来说作成一个群. 因为

Ⅰ. 两个整数相加还是一个整数;

Ⅱ. $a+(b+c)=(a+b)+c$;

Ⅲ. a,b 是整数的时候,$a+x=b$, $y+a=b$ 有整数解.

例 3 G 是所有不等于零的整数的集合. G 对于普通乘法来说不作成一个群. 因为,固然

Ⅰ. 整数乘整数还是整数,

Ⅱ. $a(bc)=(ab)c$,

但 $3x=2$ 没有整数解,Ⅲ 不能被满足.

但 G 若是全体不等于零的有理数的集合,那么 G 对于普通乘法来说作成一个群.

现在假定 G 是一个群. 我们证明 G 有以下性质.

Ⅳ. G 里至少存在一个元 e,叫做 G 的一个左单位元,能让

$$ea=a$$

对于 G 的任何元 a 都成立.

证明 由 Ⅲ,对于一个固定的元 b,

$$yb=b$$

在 G 里有解. 我们任意取一个解,叫它作 e:

(1) $$eb=b$$

我们说,对于 G 的一个任意元 a,

$$ea=a$$

成立. 由 Ⅲ, $bx=a$ 有解 c:

(2)
$$bc=a$$

由(1),(2),Ⅱ,

$$ea=e(bc)=(eb)c=bc=a$$

这样，我们证明了 e 的存在．证完．

Ⅴ．对于 G 的每一个元 a，在 G 里至少存在一个元 a^{-1}，叫做 a 的一个左逆元，能让

$$a^{-1}a=e$$

成立．这里 e 是一个固定的左单位元．

证明　由Ⅲ，$ya=e$ 可解．证完．

Ⅳ，Ⅴ两个性质非常重要，因为它们可以代替群的第一定义里的第三条．

群的第二定义　我们说，一个不空集合 G 对于一个叫做乘法的代数运算来说作成一个群，假如

Ⅰ．G 对于乘法来说是闭的；

Ⅱ．结合律成立：

$$a(bc)=(ab)c$$

对于 G 的任意三个元 a,b,c 都对；

Ⅳ．G 里至少存在一个左单位元 e，能让

$$ea=a$$

对于 G 的任何元 a 都成立；

Ⅴ．对于 G 的每一个元 a，在 G 里至少存在一个左逆元 a^{-1}，能让

$$a^{-1}a=e$$

我们已经看到，由Ⅰ，Ⅱ，Ⅲ可以推出Ⅳ，Ⅴ来．现在我们反过来证明，由Ⅰ，Ⅱ，Ⅳ，Ⅴ也可以推出Ⅲ来．这就是说，以上两个定义有同等价值．这一点我们分三步来证明．

(i)　一个左逆元一定也是一个右逆元．这句话的意思是：

由 $\qquad a^{-1}a=e$

可得 $\quad aa^{-1}=e$

因为由 V, G 有元 a', 使得

$$a'a^{-1}=e$$

所以 $\qquad (a'a^{-1})(aa^{-1})=e(aa^{-1})=(ea)a^{-1}=aa^{-1}$

但 $\quad (a'a^{-1})(aa^{-1})=a'[(a^{-1}a)a^{-1}]=a'(ea^{-1})=a'a^{-1}=e$

所以 $$aa^{-1}=e$$

(ii) 一个左单位元一定也是一个右单位元. 这就是说:

$$ae=a$$

对 G 的任何元 a 成立.

因为 $$(aa^{-1})a=ea=a$$

$$(aa^{-1})a=a(a^{-1}a)=ae$$

所以 $$ae=a$$

(iii) 现在我们证明,

$$ax=b$$

可解.

我们取 $x=a^{-1}b$. 由 V, a^{-1} 存在; 由 I, $a^{-1}b\in G$. G 的这个元显然是以上方程的解, 因为由 II, (i), 同 V,

$$a(a^{-1}b)=(aa^{-1})b=eb=b$$

同样, ba^{-1} 是

$$ya=b$$

的解. 证完.

群的第二定义应用起来常比第一个方便, 这一点应该注意.

以下我们还要说明几个名词和符号.

1. 一个群 G 的元素的个数可以有限也可以无限. 我们规定

定义 一个群叫做**有限群**, 假如这个群的元的个数是一个有限整数. 不然的话, 这个群叫做**无限群**. 一个有限群的元的个数

叫做这个**群的阶**.

上面例 1 的群是有限群，例 2，例 3 的群是无限群.

2. 在一个群里结合律是对的，所以

$$a_1a_2\cdots a_n$$

有意义，是 G 的某一个元. 这样，我们当然可以把 n 个相同的元 a 来相乘. 因为我们用普通乘法的符号来表示群的乘法，这样得来的一个元我们也用普通符号 a^n 来表示：

$$a^n=\overbrace{aa\cdots a}^{n\text{ 次}}\qquad n\text{ 是正整数}$$

并且也把它叫做 a 的 n 次乘方(简称 n 次方).

3. 在一般的群里交换律未必成立. 但在特别的群里交换律是可以成立的，比方说我们以上三个例子里的群就都有这个性质.

定义 一个群叫做**交换群**，假如

$$ab=ba$$

对于 G 的任何两个元 a,b 都成立.

习 题

1. 全体整数的集合对于普通减法来说是不是一个群？
2. 举一个有两个元的群的例.
3. 证明，我们也可以用条件 I，II 以及下面的条件 IV′，V′ 来作群的定义：

IV′. G 里至少存在一个右单位元 e，能让

$$ae=a$$

对于 G 的任何元 a 都成立；

V′. 对于 G 的每一个元 a，在 G 里至少存在一个右逆元 a^{-1}，能让

$$aa^{-1}=e$$

§2. 单位元、逆元、消去律

在这一节里我们要证明群的几个极重要的性质.

定理1 在一个群G里存在一个并且只存在一个元e，能使

$$ea=ae=a$$

对于G的任意元a都对.

证明 这样的一个e存在，我们在上节已经证明过. 假定还有一个e'也有这样的性质:

$$e'a=ae'=a, \quad (a\text{ 可以是 }G\text{ 的任意元})$$

那么

$$ee'=e=e'$$

所以G只有一个这样的e. 证完.

这个e在一个群里占一个极重要的地位.

定义 一个群G的唯一的能使

$$ea=ae=a \qquad (a\text{ 是 }G\text{ 的任意元})$$

的元e叫做群G的**单位元**.

定理2 对于群G的每一个元a来说，在G里存在一个而且只存在一个元a^{-1}，能使

$$a^{-1}a=aa^{-1}=e$$

证明 这样的一个a^{-1}存在，我们已经知道. 假定a'也是一个这样的元:

$$a'a=aa'=e$$

那么

$$a'aa^{-1}=(a'a)a^{-1}=ea^{-1}=a^{-1}$$
$$=a'(aa^{-1})=a'e=a'$$

所以只有一个这样的a^{-1}. 证完.

定义 唯一的能使

$$a^{-1}a=aa^{-1}=e$$

的元a^{-1}叫做元a的**逆元**(有时简称**逆**).

我们看两个例.

例1 我们已经知道全体不等于零的有理数对于普通乘法来

说作成一个群. 这个群的单位元是 1, a 的逆元是 $\frac{1}{a}$.

例 2 全体整数对于普通加法来说作成一个群. 这个群的单位元是零, a 的逆元是 $-a$.

当 n 是正整数时, 我们已经规定过符号 a^n 的意义, 并且我们很容易算出

$$a^n a^m = a^{n+m} \tag{1}$$

$$(a^n)^m = a^{nm} \tag{2}$$

现在我们利用唯一的单位元 e 和 a 的逆元 a^{-1} 规定:

$$a^0 = e$$

$$a^{-n} = (a^{-1})^n \qquad (n \text{ 正整数})$$

这样规定以后, 我们很容易算出, (1), (2) 两式对于任何整数 n、m 都对.

还有一个重要的概念也是利用位单元 e 来规定的.

定义 我们看群 G 的一个元 a. 能够使得

$$a^m = e$$

的最小的正整数 m 叫做 a 的阶. 若是这样的一个 m 不存在, 我们说, a 是无限阶的.

我们再举一个例.

例 3 G 刚好包含 $x^3 = 1$ 的三个根:

$$1, \quad \varepsilon_1 = \frac{-1+\sqrt{-3}}{2}, \quad \varepsilon_2 = \frac{-1-\sqrt{-3}}{2}$$

对于普通乘法来说这个 G 作成一个群.

I, II 显然;

IV. 1 是 G 的单位元;

V. 1 的逆元是 1, ε_1 的逆元是 ε_2, ε_2 的逆元是 ε_1.

在这个群里 1 的阶是 1, ε_1 的阶是 3, ε_2 的阶是 3.

群的另一个极重要的性质是

定理 3 一个群的乘法适合

III′. 消去律：若 $ax=ax'$，那么 $x=x'$；

若 $ya=y'a$，那么 $y=y'$.

证明 假定
$$ax=ax'$$
那么
$$a^{-1}(ax)=a^{-1}(ax')$$
$$(a^{-1}a)x=(a^{-1}a)x'$$
$$ex=ex'$$
$$x=x'$$
同样，由
$$ya=y'a$$
可得
$$y=y'$$
证完

推论 在一个群里，方程
$$ax=b,\quad ya=b$$
各有唯一的解.

习 题

1. 若群 G 的每一个元都适合方程 $x^2=e$，那么 G 是交换群.
2. 在一个有限群里阶大于 2 的元的个数一定是偶数.
3*. 假定 G 是一个阶是偶数的有限群. 在 G 里阶等于 2 的元的个数一定是奇数.
4. 一个有限群的每一个元的阶都有限.

§3. 有限群的另一定义

对于一个有限群我们常用到一个定义，这个定义与以上的一般定义稍微有点不同. 因为有限群在群论里占一个极重要的地位，我们对于这个定义还要讨论一下.

我们在上面已经看到，假如一个有乘法的集合适合 I，II，III，那么它一定适合 I，II，III′. 现在我们反过来问：假定一个集合适合 I，

Ⅱ,Ⅲ′,它是不是一定适合Ⅰ,Ⅱ,Ⅲ呢？回答是：不一定.

例 $G=\{$所有不等于零的整数$\}$.

对于普通乘法来说这个G适合Ⅰ,Ⅱ,Ⅲ′,可是不适合Ⅲ.

但如果G是一个有限集合时，情形就不同了. 因为我们有

定理 一个有乘法的有限集合G若是适合Ⅰ,Ⅱ和Ⅲ′, 那么它也适合Ⅲ.

证明 我们先证明，

$$ax=b$$

在G中有解.

假定G有n个元，这n个元我们用

$$a_1, a_2, \cdots, a_n$$

来表示. 我们用a从左边来乘所有的a_i而作成一个集合

$$G'=\{aa_1, aa_2, \cdots, aa_n\}$$

由于Ⅰ,
$$G'\subseteq G$$
但当$i\neq j$的时候，

$$aa_i\neq aa_j$$

不然的话，由消去律，$a_i=a_j$，与假定不合. 因此G'有n个不同的元，而

$$G'=G$$

这样，以上方程里的$b\in G'$，这就是说，

$$b=aa_k$$

a_k是以上方程的解. 同样可证，

$$ya=b$$

可解. 证完.

由这个定理我们可以得到

有限群的另一定义 我们说，一个有乘法的有限不空集合G作成一个群，假如Ⅰ,Ⅱ,Ⅲ′能被满足.

由上面的例，我们知道，这个定义所要求的条件比一般群的定义所要求的要少一点．所以在证明一个有限集合是一个群时，这个定义是一个很有力的工具．至于这个定义不能用到无限集合上去，由上面同一例可以知道．

我们知道，一个有限集合的代数运算常用一个表来表明．一个有限群的乘法若用表来表明，那么许多群的性质都可以直接从表上看出．单位元的存在告诉我们，表里一定有一行元同横线上的元一样，也一定有一列元同垂线左边的元一样．消去律告诉我们，群的全体的元必在每一行也必在每一列里出现．所以给了一个有限集合，一个代数运算，若是我们列出表来一看，以上条件不合，就知道这个集合不作成一个群．可惜结合律在表中不易看出．

§4. 群的同态

我们已经有了群的定义，并且知道了群的几个最基本的性质．现在我们要看一看，同态这一个概念在群上的应用，以便以后可以随时把一个集合来同一个群比较，或把两个群来比较．

我们假定 G 是一个群，$\bar{G}$ 是一个不空集合，并有一个代数运算．这个代数运算我们也把它叫做乘法，也用普通表示乘法的符号来表示．$\bar{G}$ 的乘法当然同 G 的乘法一般是完全不同的法则．我们把不同的法则都叫做乘法，并且用同一的符号来表示，似乎很容易弄乱．实际上，因为 G 的乘法只能应用到 G 的元上去，$\bar{G}$ 的乘法只能应用到 $\bar{G}$ 的元上去，而 G 同 $\bar{G}$ 的元的表示方法是有区别的，因此弄乱这一点是不致发生的．

现在我们证明

定理 1 假定 G 与 $\bar{G}$ 对于它们的乘法来说同态，那么 $\bar{G}$ 也是一个群．

证明 $\bar{G}$ 显然适合群定义的条件 I．G 的乘法适合结合律，而 G 与 $\bar{G}$ 同态，由§8，定理 1，$\bar{G}$ 的乘法也适合结合律，所以 $\bar{G}$ 适合群定义的条件 II．我们证明 $\bar{G}$ 也适合 IV，V 两条．

IV．G 有单位元 e．在所给同态满射之下，e 有象 $\bar{e}$：

$$e \longrightarrow \bar{e}$$

我们说，$\bar{e}$ 就是 $\bar{G}$ 的一个左单位元．假定 $\bar{a}$ 是 $\bar{G}$ 的任意元，而 a 是 $\bar{a}$ 的一个逆象：

$$a \longrightarrow \bar{a}$$

那么
$$ea \longrightarrow \bar{e}\bar{a}$$

但
$$ea = a$$

所以
$$\bar{e}\bar{a} = \bar{a}$$

V．假定 $\bar{a}$ 是 $\bar{G}$ 的任意元，a 是 $\bar{a}$ 的一个逆象：

$$a \longrightarrow \bar{a}$$

a 是群 G 的元，a 有逆元 a^{-1}．我们把 a^{-1} 的象叫做 $\overline{a^{-1}}$：

$$a^{-1} \longrightarrow \overline{a^{-1}}$$

那么
$$a^{-1}a \longrightarrow \overline{a^{-1}}\bar{a}$$

但
$$a^{-1}a = e \longrightarrow \bar{e}$$

所以
$$\overline{a^{-1}}\bar{a} = \bar{e}$$

这就是说，$\overline{a^{-1}}$ 是 $\bar{a}$ 的左逆元，也就是 $\bar{a}$ 的逆元．证完．

我们举一个例．

例 1 A 包含 a、b、c 三个元．A 的乘法由下表规定：

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

这就是 I，4，习题 3 的那个集合．当初我们要证明 A 的代数运算

适合结合律相当费事. 现在我们要进一步证明, A 作成一个群.

由Ⅱ, 1, 例2, 我们知道, 全体整数对于普通加法来说作成一个群 G. 我们把 A 同 G 来比较一下. 作一个映射

$$\phi: \quad x \longrightarrow a, \text{ 假如 } x \equiv 0 \quad (3)$$
$$x \longrightarrow b, \text{ 假如 } x \equiv 1 \quad (3)$$
$$x \longrightarrow c, \text{ 假如 } x \equiv 2 \quad (3)$$

ϕ 显然是一个满射. 我们证明, ϕ 是一个同态满射. 首先要注意, G 和 A 的代数运算都是适合交换律的, 所以只要 $x+y \longrightarrow \bar{x}\bar{y}$, 那么 $y+x \longrightarrow \bar{y}\bar{x}$. 所以要看 ϕ 是不是同态满射, 测验了 $x+y$ 的情形, 就不必再测验 $y+x$ 的情形. 现在我们分六个情形来测验.

(i) $x \equiv 0 \quad (3), \quad y \equiv 0 \quad (3)$

那么 $$x+y \equiv 0 \quad (3)$$

这样, $$x \longrightarrow a, \quad y \longrightarrow a$$
$$x+y \longrightarrow a \quad aa$$

(ii) $x \equiv 0 \quad (3), \quad y \equiv 1 \quad (3)$

那么 $$x+y \equiv 1 \quad (3)$$

这样, $$x \longrightarrow a, \quad y \longrightarrow b$$
$$x+y \longrightarrow b = ab$$

(iii) $x \equiv 0 \quad (3), \quad y \equiv 2 \quad (3)$

那么 $$x+y \equiv 2 \quad (3)$$

这样, $$x \longrightarrow a, \quad y \longrightarrow c$$
$$x+y \longrightarrow c = ac$$

(iv) $x \equiv 1 \quad (3), \quad y \equiv 1 \quad (3)$

那么 $$x+y \equiv 2 \quad (3)$$

这样, $$x \longrightarrow b, \quad y \longrightarrow b$$
$$x+y \longrightarrow c = bb$$

(v) $x \equiv 1 \quad (3), \quad y \equiv 2 \quad (3)$

那么 $$x+y\equiv 0\quad(3)$$

这样， $$x\longrightarrow b,\quad y\longrightarrow c$$

$$x+y\longrightarrow a=bc$$

(vi) $x\equiv 2\quad(3)$, $y\equiv 2\quad(3)$

那么 $$x+y\equiv 1\quad(3)$$

这样， $$x\longrightarrow c,\quad y\longrightarrow c$$

$$x+y\longrightarrow b=cc$$

这样 G 与 A 同态，A 是一个群.

我们要注意，假如 G 同 $\bar{G}$ 的次序掉换一下，那么定理 1 不一定对，换一句话说，假如 $\bar{G}$ 与 G 同态，那么 $\bar{G}$ 不一定是一个群.

例 2 $\bar{G}=\{$所有奇数$\}$. $\bar{G}$ 对于普通乘法来说不作成一个群. $G=\{e\}$. G 对于乘法 $ee=e$ 来说显然作成一个群（参看 Ⅱ，1，例 1）.

但 $$\phi:\ \bar{a}\longrightarrow e$$

显然是 $\bar{G}$ 到 G 的一个同态满射.

当然在我们考虑之下的映射若是一个同构映射，G 同 $\bar{G}$ 的次序就没有关系了.

以下我们若是说两个群 G 与 $\bar{G}$ 同态（同构），我们的意思永远是：它们对于一对群乘法来说同态（同构）.

由定理 1 的证明我们直接可以看出

定理 2 假定 G 和 $\bar{G}$ 是两个群. 在 G 到 $\bar{G}$ 的一个同态满射之下，G 的单位元 e 的象是 $\bar{G}$ 的单位元，G 的元 a 的逆元 a^{-1} 的象是 a 的象的逆元.

在 G 与 $\bar{G}$ 间的一个同构映射之下，两个单位元互相对应，互相对应的元的逆元互相对应.

习　题

假定在两个群 G 和 $\bar{G}$ 的一个同态映射之下,

$$a \longrightarrow \bar{a}$$

a 与 $\bar{a}$ 的阶是不是一定相同?

§5. 变换群

我们到现在为止已经有了几个群的例子. 但这些例子或是利用普通数和普通加法乘法来作成的, 或是些极简单的, 阶只是 1, 2 或 3 的抽象群, 并且这些群都是交换群. 在这一节里我们要讨论一种具体的群. 这种群一方面本身非常重要, 另一方面它能给我们一个非交换群的例子, 并且表明, 一个群的元素不一定是数.

我们取一个集合 A. 在 I,7 我们已经规定了什么叫做 A 的一个变换: A 的一个变换, 就是一个 A 到 A 自己的映射. 用说明一般映射的符号来说明一个变换 τ, 应该是

τ: $$a \longrightarrow a' = \tau(a)$$

但现在为便利起见, 对于变换这一种特殊的映射要用一种特殊的符号来说明. 我们用符号

τ: $$a \longrightarrow a' = a^{\tau}$$

a^{τ} 当然不是 a 的 τ 次方的意思, 因为 τ 是一个变换, a 的 τ 次方根本没有什么意义. 这只是一个符号, 正如我们对于特殊的映射: 代数运算以及关系都用特殊的符号一样. 一个集合 A 在一般情形之下当然可以有若干个不同的变换, 我们再举一个简单的例.

例 1　$A = \{1, 2\}$.

τ_1: $1 \longrightarrow 1$, $2 \longrightarrow 1$

τ_2: $1 \longrightarrow 2$, $2 \longrightarrow 2$

τ_3: $\qquad 1 \longrightarrow 1, \quad 2 \longrightarrow 2$

τ_4: $\qquad 1 \longrightarrow 2, \quad 2 \longrightarrow 1$

是 A 的所有的变换．其中 τ_3, τ_4 是一一变换．

现在我们把给定的一个集合 A 的全体变换放在一起，作成一个集合

$$S = \{\tau, \lambda, \mu, \cdots\}$$

我们要想法规定一个 S 的代数运算，这个代数运算我们把它叫做乘法．我们看 S 的两个元 τ 和 λ，

$$\tau: \quad a \longrightarrow a^{\tau}, \qquad \lambda: \quad a \longrightarrow a^{\lambda}$$

那么

$$a \longrightarrow (a^{\tau})^{\lambda}$$

显然也是 A 的一个变换．因为给了 A 的任意元 a，我们可以得出一个唯一的 $(a^{\tau})^{\lambda}$ 来．现在我们规定，就把这个变换叫做 τ 同 λ 的乘积，

$\tau\lambda$: $\qquad a \longrightarrow (a^{\tau})^{\lambda} = a^{\tau\lambda}$

这样，这个乘法是一个 S 的代数运算．我们举一个例．

例 2 我们在例 1 里取几个变换来算一算它们的乘积．

$\tau_1\tau_2$: $\qquad 1 \longrightarrow$ [illegible]$, \quad$ [illegible] $\longrightarrow 2$

所以 $\qquad \tau_1\tau_2 = \tau_2$

$\tau_2\tau_4$: $\qquad 1 \longrightarrow 1, \quad 2 \longrightarrow 1$

所以 $\qquad \tau_2\tau_4 = \tau_1$

我们说，如上规定的乘法适合结合律：

$$\tau(\lambda\mu) = (\tau\lambda)\mu$$

因为

$\tau(\lambda\mu)$: $\qquad a \longrightarrow (a^{\tau})^{\lambda\mu} = \{(a^{\tau})^{\lambda}\}^{\mu}$

$(\tau\lambda)\mu$: $\qquad a \longrightarrow (a^{\tau\lambda})^{\mu} = \{(a^{\tau})^{\lambda}\}^{\mu}$

对于这个乘法来说，S 有一个单位元，就是 A 的恒等变换

e: $\qquad a \longrightarrow a$

因为

$\varepsilon\tau$: $$a \longrightarrow (a^{\varepsilon})^{\tau} = a^{\tau}$$

$$\varepsilon\tau = \tau$$

$\tau\varepsilon$: $$a \longrightarrow (a^{\tau})^{\varepsilon} = a^{\tau}$$

$$\tau\varepsilon = \tau$$

这样，S 对于这个乘法来说差不多已经作成一个群了．可惜，虽然说是差不多，到底还是差一点．因为一个任意的变换 τ 不一定有一个逆元．

例 3 我们看例 1 里的 τ_1．用一个任意的 τ 从左边来乘 τ_1，得到

$\tau\tau_1$: $$1 \longrightarrow (1^{\tau})^{\tau_1} = 1, \quad 2 \longrightarrow (2^{\tau})^{\tau_1} = 1$$

这就是说，不管 τ 是 A 的哪一个变换，

$$\tau\tau_1 \neq \varepsilon$$

换一句话说，τ_1 没有逆元．

这样，一般 S 不作成一个群．

S 本身虽然一般不作成一个群，但它的一个子集 G 对于上述乘法来说却不见得不能作成一个群．让我们先看一看 G 作成一个群的必要条件．

定理 1 假定 G 是集合 A 的若干个变换所作成的集合，并且 G 包含恒等变换 ε．若是对于上述乘法来说 G 作成一个群，那么 G 只包含 A 的一一变换．

证明 令 τ 是 G 的任意元，那么因为 G 是群，有 τ^{-1}，使得

$$\tau^{-1}\tau = \tau\tau^{-1} = \varepsilon$$

我们现在证明 τ 是 A 的一一变换．我们已经知道，τ 是 A 的变换，这就是说，τ 是一个 A 到 A 的映射．在 A 里取任意元 a，那么

τ: $$a^{\tau^{-1}} \longrightarrow (a^{\tau^{-1}})^{\tau} = a^{\tau^{-1}\tau} = a^{\varepsilon} = a$$

所以 τ 是 A 到 A 的满射．假定

$$a^{\tau} = b^{\tau}$$

那么
$$(a^{\tau})^{\tau^{-1}}=(b^{\tau})^{\tau^{-1}}$$
$$a^{\varepsilon}=b^{\varepsilon}$$
$$a=b$$
所以 τ 是 A 与 A 间的一一映射. 这就是说, τ 是 A 的一一变换. 证完.

现在我们规定

定义 一个集合 A 的若干个一一变换对于以上规定的乘法作成的一个群叫做 A 的一个**变换群**.

以上我们得到了变换作成群的必要条件, 并且按照这个条件规定了变换群这个名词. 但变换群是不是存在, 换一句话说, 我们是不是找得到若干个一一变换, 使得它们作成一个群, 我们还不知道. 事实上这种群是有的.

定理 2 一个集合 A 的所有的一一变换作成一个变换群 G.

证明 G 适合群定义的 I, II, IV, V 四个条件.

I. 假如 τ_1, τ_2 是一一变换, 那么 $\tau_1\tau_2$ 也是.

因为在 A 里取一个任意元 a, 由于 τ_2 是一一变换, 在 A 里有 a' 有以下性质,

τ_2: $$a'\longrightarrow a=a'^{\tau_2}$$
由于 τ_1 是一一变换, 在 A 里有 a'' 有以下性质,

τ_1: $$a''\longrightarrow a'=a''^{\tau_1}$$
这样,

$\tau_1\tau_2$: $$a''\longrightarrow(a''^{\tau_1})^{\tau_2}=a'^{\tau_2}=a$$
所以 $\tau_1\tau_2$ 是 A 到 A 的满射. 假如 $a\neq b$, 那么
$$a^{\tau_1}\neq b^{\tau_1},\quad (a^{\tau_1})^{\tau_2}\neq(b^{\tau_1})^{\tau_2}$$
$$a^{\tau_1\tau_2}\neq b^{\tau_1\tau_2}$$
所以 $\tau_1\tau_2$ 是一一变换.

II. 结合律对于一般的变换都对, 所以对于一一变换也对.

Ⅳ. e 是一一变换.

Ⅴ. 设 τ 是一个任意的一一变换，那么由1,7，有一个一一变换 τ^{-1}，有以下性质，

τ^{-1}: $a\longrightarrow a^{\tau^{-1}}$， 假如 $(a^{\tau^{-1}})^{\tau}=a$

所以

$\tau^{-1}\tau$: $a\longrightarrow (a^{\tau^{-1}})^{\tau}=a$

$$\tau^{-1}\tau=\varepsilon$$

证完

这样，我们证明了变换群的确是存在的. 这也是我们第一次碰到的元素不是数的具体群. 以上的定理当然不是说，除了全体一一变换所作成的集合以外，没有其它的变换群存在.

例4 假如 A 是一个平面的所有的点作成的集合，那么平面的一个绕一个定点的旋转可以看成 A 的一个一一变换. 我们叫 G 包含所有绕一个定点的旋转，那么 G 作成一个变换群. 因为假如我们用 τ_θ 来表示转 θ 角的旋转，就有

Ⅰ. $\tau_{\theta_1}\tau_{\theta_2}=\tau_{\theta_1+\theta_2}$，$G$ 是闭的；

Ⅱ. 结合律当然成立；

Ⅳ. $e=\tau_0\in G$；

Ⅴ. $\tau_\theta^{-1}=\tau_{-\theta}$.

但 G 显然不包括 A 的全部一一变换.

所以给了一个集合 A，除了定理2的最大的变换群以外，A 的确还可以有别的较小的变换群.

变换群一般不是交换群. 假如 τ_1 是平面的一个平移，它把原点(0,0)平移到(1,0)；τ_2 是绕原点转 $\frac{\pi}{2}$ 的旋转，那么 τ_1 和 τ_2 都是例4的集合 A 的一一变换. 但

$\tau_1\tau_2$: $(0,0)\longrightarrow(0,1)$

$\tau_2\tau_1$: $(0,0)\longrightarrow(1,0)$

$$\tau_1\tau_2 \neq \tau_2\tau_1$$

这样，变换群告诉我们非交换群的存在。

变换群在数学上，尤其在几何上的实际应用极广。但就是在群的理论上这种群也有它的重要性。我们有

定理 3 任何一个群都同一个变换群同构。

证明 假定 G 是一个群，G 的元是 $a, b, c, \cdots$。我们在 G 里任意取出一个元 x 来，那么

τ_x: $$g \longrightarrow gx = g^{\tau_x}$$

是集合 G 的一个变换。因为给了 G 的任意元 g，我们能够得到一个唯一的 G 的元 g^{τ_x}。这样由 G 的每一个元 x，可以得到 G 的一个变换 τ_x。我们把所有这样得来的 G 的变换放在一起，作成一个集合 $\bar{G} = \{\tau_a, \tau_b, \tau_c, \cdots\}$。那么

ϕ: $$x \longrightarrow \tau_x$$

是 G 到 $\bar{G}$ 的满射。但消去律：$x \neq y \Longrightarrow gx \neq gy$ 告诉我们，

$$\text{若 } x \neq y\text{，那么 } \tau_x \neq \tau_y$$

所以 ϕ 是 G 与 $\bar{G}$ 间的一一映射。再进一步看，

$$g^{\tau_{xy}} = g(xy) = (gx)y = (g^{\tau_x})y = (g^{\tau_x})^{\tau_y} = g^{\tau_x\tau_y}$$

这就是说，
$$\tau_x\tau_y = \tau_{xy}$$

所以 ϕ 是 G 与 $\bar{G}$ 间的同构映射，所以 $\bar{G}$ 是一个群。但 G 的单位元 e 的象

τ_e: $$g \longrightarrow ge = g$$

是 G 的恒等变换 ε，由本节定理 1，$\bar{G}$ 是 G 的一个变换群。这样 G 与 G 的一个变换群 $\bar{G}$ 同构。证完。

这个定理告诉我们，任意一个抽象群都能够在变换群里找到一个具体的实例。换一句话说，我们不必害怕，以后会找得到一个抽象群，这个群完全是我们的脑子造出来的空中楼阁。

习　题

1.*假定 τ 是集合 A 的一个非一一变换. τ 会不会有一个左逆元 τ^{-1}, 使得 $\tau^{-1}\tau=\varepsilon$?

2. 假定 A 是所有实数作成的集合. 证明, 所有 A 的可以写成

$$x \longrightarrow ax+b, \quad a, b \text{ 是有理数}, a \neq 0$$

形式的变换作成一个变换群. 这个群是不是一个交换群?

3. 假定 S 是一个集合 A 的所有变换作成的集合. 我们暂时仍用旧符号

$$\tau: \qquad a \longrightarrow a' = \tau(a)$$

来说明一个变换 τ. 证明, 我们可以用

$$\tau_1\tau_2: \qquad a \longrightarrow \tau_1[\tau_2(a)] = \tau_1\tau_2(a)$$

来规定一个 S 的乘法, 这个乘法也适合结合律, 并且对于这个乘法来说 ε 还是 S 的单位元.

4. 证明, 一个变换群的单位元一定是恒等变换.

5. 证明, 实数域上一切有逆的 $n\times n$ 矩阵对于矩阵乘法来说, 作成一个群.

§6. 置换群

变换群的一种特例, 叫做置换群, 在代数里占一个很重要的地位. 比方说, 在解决方程能不能用根号解这个问题时就要用到这种群. 这种群还有一个特点, 就是它们的元可以用一种很具体的符号来表示, 使得在这种群里的计算比较简单. 现在我们把这种群讨论一下.

定义 一个有限集合的一个一一变换叫做一个置换.

一个有限集合的若干个置换作成的一个群叫做一个置换群.

我们看一个有限集合 A, A 有 n 个元 $a_1, a_2, \cdots, a_n$. 由 I, 5, 定理 2, A 的全体置换作成一个群 G.

定义 一个包含 n 个元的集合的全体置换作成的群叫做 n 次

对称群. 这个群我们用 S_n 来表示.

由初等代数我们知道，n 个元的置换一共有 $n!$ 个. 这也很容易证明，我们要作 n 个元的一个置换，就是要替每一个元选定一个对象，我们替 a_1 选定对象时，有 n 个可能，选定了以后，再替 a_2 选时，就只有 $n-1$ 个可能，这样下去，一共可以得到

$$n(n-1)\cdots 2\cdot 1=n!$$

个不同的置换. 这样，我们有

定理 1 n 次对称群 S_n 的阶是 $n!$.

现在我们要看一看表示一个置换的符号. 这种符号普通有两种，我们先说明第一种. 我们看一个置换

π: $$a_i \longrightarrow a_{k_i},\quad i=1,2,\cdots,n$$

这样一个置换所发生的作用完全可以由 $(1,k_1),(2,k_2),\cdots,(n,k_n)$ 这 n 对整数来决定. 我们表示置换的第一个方法就是把以上这个置换写成

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

在这种表示方法里，第一行的 n 个数字的次序显然没有什么关系，比方说以上的 π 我们也可用

$$\begin{pmatrix} 2 & 1 & 3 & \cdots & n \\ k_2 & k_1 & k_3 & \cdots & k_n \end{pmatrix}$$

来表示. 不过我们用到最多的还是 $1,2,\cdots,n$ 这个次序，其它次序只有在有必要时才用. 我们举一个例.

例 1. $n=3$. 这时我们有 $1,2,3$ 三个数字. 我们可以给它们六种不同的次序，所以每一个置换也有六种不同的表示方法. 假如

π: $$a_1 \longrightarrow a_2,\quad a_2 \longrightarrow a_3,\quad a_3 \longrightarrow a_1$$

那么

$$\pi=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&3&2\\2&1&3\end{pmatrix}=\begin{pmatrix}2&1&3\\3&2&1\end{pmatrix}=\begin{pmatrix}2&3&1\\3&1&2\end{pmatrix}=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}=\begin{pmatrix}3&2&1\\1&3&2\end{pmatrix}$$

不过我们普通用$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$来表示这个 π.

以上的表示方法不仅是一个符号. 因为不管上一行的 n 个数字的次序如何，这样一个符号都能具体地告诉我们，它所表示的置换 π 是怎样的一个置换；换一句话说，它能告诉我们，经过这个 π，某一个元 a_i 的象是什么，我们只须在上一行把 i 找到，然后看一看 i 底下是一个什么数字就行了. 因此，利用这种符号可以直接来计算两个置换的乘积. 我们举一个例.

例 2 由定理 1 我们知道 S_3 有 6 个元. 这 6 个元可以写成

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

让我们算一算，S_3 是不是交换群. 我们取第二个和第三个元来看一看.

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

所以 S_3 不是交换群.

无限非交换群我们已经看到过，这是我们的第一个有限非交换群的例子. S_3 可以说是一个最小的有限非交换群，因为以后我们会知道，一个有限非交换群至少要有六个元.

为了说明置换的第二种表示法，我们先证明一个公式. 看两个特殊的置换 π_1, π_2:

$$\pi_1=\begin{pmatrix}j_1\cdots j_k & j_{k+1}\cdots j_n\\ j_1^{(1)}\cdots j_k^{(1)} & j_{k+1}\cdots j_n\end{pmatrix},\quad \pi_2=\begin{pmatrix}j_1\cdots j_k & j_{k+1}\cdots j_n\\ j_1\cdots j_k & j_{k+1}^{(2)}\cdots j_n^{(2)}\end{pmatrix}$$

那么以下公式成立：

$$(1) \qquad \pi_1\pi_2 = \begin{pmatrix} j_1 & \cdots j_k & j_{k+1} \cdots j_n \\ j_1^{(1)} & \cdots j_k^{(1)} & j_{k+1}^{(2)} \cdots j_n^{(2)} \end{pmatrix}$$

要证明这个公式，我们只须注意，因为 π_1 是 $a_{j_1}, a_{j_2}, \cdots, a_{j_n}$ 这 n 个元的一一变换，而在 π_1 之下，$a_{j_{k+1}}, \cdots, a_{j_n}$ 已经各是 $a_{j_{k+1}}, \cdots, a_{j_n}$ 的象，所以它们不能再是 a_{j_i} $(i \leqslant k)$ 的象，这就是说，

当 $i \leqslant k$ 时，$$j_i^{(1)} = j_l, \quad l \leqslant k$$

这样，

当 $i \leqslant k$ 时，$$a_{j_i}^{\pi_1\pi_2} = (a_{j_i}^{\pi_1})^{\pi_2} = (a_{j_l})^{\pi_2} = a_{j_l} = a_{j_i^{(1)}}$$

当 $i > k$ 时，$$a_{j_i}^{\pi_1\pi_2} = (a_{j_i}^{\pi_1})^{\pi_2} = a_{j_i}^{\pi_2} = a_{j_i^{(2)}}$$

现在我们规定一个新的符号.

定义 S_n 的一个把 a_{i_1} 变到 a_{i_2}，a_{i_2} 变到 a_{i_3}，…，a_{i_k} 变到 a_{i_1}，而使得其余的元（假如还有的话）不变的置换，叫做一个 ***k*-循环置换**. 这样的一个置换我们用符号

$$(i_1 i_2 \cdots i_k),\ (i_2 i_3 \cdots i_k i_1),\ \cdots \text{或} (i_k i_1 \cdots i_{k-1})$$

来表示.

例 3 我们看 S_5. 这里

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5) = (2\ 3\ 4\ 5\ 1) = \cdots = (5\ 1\ 2\ 3\ 4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1) = (2) = (3) = (4) = (5)$$

一个任意的置换当然不一定是一个循环置换.

例 4 S_4 的 $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ 就不是一个循环置换. π 使得每一个元都发生变动，因此，假如 π 是一个循环置换，它一定是一个 4-循环置换. 但 π 使 $a_1 \longrightarrow a_2 \longrightarrow a_1$，所以它不会是一个 4-循环

置换. 实际上 π 是两个循环置换的乘积. 由公式 (1)，我们知道

$$\pi=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(1\ 2)(3\ 4)$$

一般来说，我们有

定理 2 每一个 n 个元的置换 π 都可以写成若干个互相没有共同数字的(不相连的)循环置换的乘积.

证明 我们用归纳法. 当 π 不使任何元变动的时候，就是当 π 是恒等置换的时候，定理是对的. 假定对于最多变动 $r-1(r\leqslant n)$ 个元的 π 定理是对的. 现在我们看一个变动 r 个元的 π. 我们任意取一个被 π 变动的元 a_{i_1}，从 a_{i_1} 出发我们找 a_{i_1} 的象 a_{i_2}，a_{i_2} 的象 a_{i_3}，这样找下去，直到我们第一次找到一个 a_{i_k} 为止，这个 a_{i_k} 的象不再是一个新的元，而是我们已经得到过的一个元：$a_{i_k}^{\pi}=a_{i_j}$，$j\leqslant k$. 因为我们一共只有 n 个元，这样的 a_{i_k} 是一定存在的. 我们说，$a_{i_k}^{\pi}=a_{i_1}$. 因为 $a_{i_j}(2\leqslant j\leqslant k)$ 已经是 $a_{i_{j-1}}$ 的象，不能再是 a_{i_k} 的象. 这样，我们得到

$$a_{i_1}\longrightarrow a_{i_2}\longrightarrow\cdots\longrightarrow a_{i_k}\longrightarrow a_{i_1}$$

因为 π 只使 r 个元变动，$k\leqslant r$. 假如 $k=r$，π 本身已经是一个循环置换，我们用不着再证明什么. 假如 $k<r$，由公式(1)，

$$\pi=\begin{pmatrix}i_1\ i_2\cdots i_k\ i_{k+1}\cdots i_r\ i_{r+1}\cdots i_n\\ i_2\ i_3\cdots i_1\ i'_{k+1}\cdots i'_r\ i_{r+1}\cdots i_n\end{pmatrix}$$

$$=\begin{pmatrix}i_1\ i_2\cdots i_k\ i_{k+1}\cdots i_r\ i_{r+1}\cdots i_n\\ i_2\ i_3\cdots i_1\ i_{k+1}\cdots i_r\ i_{r+1}\cdots i_n\end{pmatrix}\begin{pmatrix}i_1\cdots i_k\ i_{k+1}\cdots i_r\ i_{r+1}\cdots i_n\\ i_1\cdots i_k\ i'_{k+1}\cdots i'_r\ i_{r+1}\cdots i_n\end{pmatrix}$$

$$=(i_1\ i_2\cdots i_k)\pi_1$$

但 π_1 只使得 $r-k<r$ 个元变动，照归纳法的假定，可以写成不相连的循环置换的乘积：

$$\pi_1=\eta_1\eta_2\cdots\eta_m$$

在这些 η 里，$i_1, i_2, \cdots, i_k$ 不会出现．不然的话，

$$\eta_j = (\cdots i_p\, i_q \cdots), \qquad p \leqslant k$$

那么 i_p 同 i_q 不会再在其余的 η 中出现，π_1 也必使 $a_{i_p} \longrightarrow a_{i_q}$，但我们知道，$\pi_1$ 使得 a_{i_p} 不动，这是一个矛盾．这样，π 是不相连的循环置换的乘积：

$$\pi = (i_1\, i_2 \cdots i_k)\,\eta_1 \eta_2 \cdots \eta_m$$ 证完

把一个置换写成不相连的循环置换的乘积是我们表示置换的第二种方法．

例 5 S_4 的全体元用循环置换的方法写出来是

(1)；

(1 2)，(3 4)，(1 3)，(2 4)，(1 4)，(2 3)；

(1 2 3)，(1 3 2)，(1 3 4)，(1 4 3)，(1 2 4)，(1 4 2)，(2 3 4)，(2 4 3)；

(1 2 3 4)，(1 2 4 3)，(1 3 2 4)，(1 3 4 2)，(1 4 2 3)，(1 4 3 2)；

(12)(34)，(13)(24)，(14)(23)．

用循环置换来表示置换的方法比第一种方法简单，并且能告诉我们每一个置换的特性．比方说，在例 5 里我们可以由于这种表示方法看出，S_4 的元可以分成五类，每一类的元的性质一定相同．所以计算置换群用第二种方法的时候比较多．当然在特殊情形之下，也有用第一种方法比较方便的时候．由于 Ⅱ，5，定理 3，我们有

定理 3 每一个有限群都与一个置换群同构．

这就是说，每一个有限群都可以在置换群里找到例子．现在置换群又是一种比较容易计算的群，所以用置换群来举有限群的例是最合理的事．

习　题

1．找出所有 S_3 的不能和 $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ 交换的元．

2. 把 S_3 的所有的元写成不相连的循环置换的乘积.

3. 证明:

(i) 两个不相连的循环置换可以交换;

(ii) $(i_1i_2\cdots i_k)^{-1}=(i_ki_{k-1}\cdots i_1)$

4. 证明一个 k-循环置换的阶是 k.

5. *证明 S_n 的每一个元都可以写成

$$(12),(13),\cdots,(1n)$$

这 $n-1$ 个 2-循环置换中的若干个的乘积.

§7. 循环群

以上我们认识了两种具体的群. 但具体的群多得很, 是研究不完的. 所以我们现在又要反回来讨论一般的抽象群. 依照上两节的定理, 如果我们能把变换群完全研究清楚, 那就等于把全体抽象群都研究清楚了; 如果能把置换群完全研究清楚, 也就等于把全体有限群都研究清楚了. 但经验告诉我们, 研究变换群或置换群并不比研究抽象群容易. 所以研究抽象群一般还是用的直接方法.

研究群的最大目的可以用一句话说完, 就是要把所有的抽象群都找出来. 说详细一点,就是要看一看,一共有多少个互相不同构的群存在. 因为能够达到这个目的, 那么所有的群就都已经在我们掌握里面,群论就可以告一结束. 为达到这个目的,我们并不企图一下子就把所有的群都找出来. 因为否则问题太复杂了. 我们的方法是:把群分成若干类,比方说,有限群,无限群,交换群,非交换群等等,然后看一看,每一类有多少不同的群. 可惜到现在为止,我们对于群的知识还是有限得很,已经完全弄清楚了的群只有少数几类, 其余大多数的群还在等待我们去解决. 在这一节里我们要把已经完全解决了的一类群讨论一下.

看一个群 G. 我们问 G 的元会不会都是 G 的某一个固定元 a 的乘方？我们说这个情形是可能的.

例 1 G 是所有整数的集合. 我们知道 G 对于普通加法来说作成一个群. 这个群我们以下把它叫做**整数加群**. 这个群的全体的元就都是 1 的乘方. 这一点，假如把 G 的代数运算不用 $+$ 而用 $\circ$ 来表示，就很容易看出. 我们知道 1 的逆元是 -1. 假定 m 是任意正整数，那么

$$m=\overbrace{1+1+\cdots+1}^{m}=\overbrace{1\circ 1\circ\cdots\circ 1}^{m}=1^m$$

$$-m=\overbrace{(-1)+(-1)+\cdots+(-1)}^{m}=\overbrace{(-1)\circ(-1)\circ\cdots\circ(-1)}^{m}=1^{-m}$$

这样 G 的不等于零的元都是 1 的乘方. 但 0 是 G 的单位元，照定义

$$0=1^0$$

现在我们规定

定义 若一个群 G 的每一个元都是 G 的某一个固定元 a 的乘方，我们就把 G 叫做**循环群**；我们也说，G 是由元 a 所生成的，并且用符号

$$G=(a)$$

来表示. a 叫做 G 的一个**生成元**.

我们再举一个例.

例 2 G 包含模 n 的 n 个剩余类. 我们要规定一个 G 的代数运算. 这一次我们把这个代数运算叫做加法，并用普通表示加法的符号来表示. 跟从前一样，我们用 $[a]$ 来表示 a 这个整数所在的剩余类. 我们规定：

(1) $$[a]+[b]=[a+b]$$

我们先要看一看，这样规定的 $+$ 是不是一种代数运算. 我们知道，

假如 $a'\in[a]$, $b'\in[b]$

那么 $[a']=[a]$, $[b']=[b]$

照我们的规定，

(2) $$[a']+[b']=[a'+b']$$

(1),(2)两式的左端是一样的,如果它们的右端不一样:

$$[a+b]\neq[a'+b']$$

那么我们规定的+就不是一种代数运算了. 我们说，这种情形不会发生. 因为

$$[a']=[a],\quad [b']=[b]$$

就是说 $a'\equiv a\ (n)$, $b'\equiv b\ (n)$

也就是说 $n|a'-a$, $n|b'-b$

因此， $n|(a'-a)+(b'-b)$

$$n|(a'+b')-(a+b)$$

这就是说

$$[a'+b']=[a+b]$$

这样,规定的+是一个 G 的代数运算. 但

$$[a]+([b]+[c])=[a]+[b+c]=[a+(b+c)]=[a+b+c]$$

$$([a]+[b])+[c]=[a+b]+[c]=[(a+b)+c]=[a+b+c]$$

这就是说 $[a]+([b]+[c])=([a]+[b])+[c]$

并且 $[0]+[a]=[0+a]=[a]$

$$[-a]+[a]=[-a+a]=[0]$$

所以对于这个加法来说， G 作成一个群. 这个群叫做模 n 的剩余类加群.

我们以前说过，普通我们用 $0,1,2,\cdots,n-1$ 来作模 n 的 n 个剩余类的全体代表团. 所以普通也用$[0]$, $[1]$, $\cdots$, $[n-1]$来表示这 n 个剩余类. 现在我们就用这 n 个固定的符号来作群 G 的一个运算表,使得我们对于这个群有一个更清楚的印象:

	[0]	[1]	⋯	[$n-2$]	[$n-1$]
[0]	[0]	[1]	⋯	[$n-2$]	[$n-1$]
[1]	[1]	[2]	⋯	[$n-1$]	[0]
⋮	⋯	⋯	⋯	⋯	⋯
[$n-1$]	[$n-1$]	[0]	⋯	[$n-3$]	[$n-2$]

这样得到的剩余类加群是循环群，因为[1]显然是G的一个生成元：G的每一个元可写成

$$[i],\quad 1\leqslant i\leqslant n$$

的样子，这样的一个元

$$[i]=\overbrace{[1]+[1]+\cdots+[1]}^{i}$$

我们以上给了两种循环群的例子．这两个例子并不是随意选的．实际上，由于这两个例子我们已经认识了所有的循环群．因为我们有

定理 假定G是一个由元a所生成的循环群．那么G的构造完全可以由a的阶来决定：

a的阶若是无限，那么G与整数加群同构；

a的阶若是一个有限整数n，那么G与模n的剩余类加群同构．

证明 第一个情形：a的阶无限．这时，

$$a^h=a^k,\ \text{当而且只当}\ h=k\ \text{的时候}.$$

由$h=k$，可得$a^h=a^k$．显然．假如$a^h=a^k$而$h\neq k$，我们可以假定$h>k$，而得到$a^{h-k}=e$，与a的阶是无限的假定不合．

这样，

$$a^k\longrightarrow k$$

是G与整数加群$\bar{G}$间的一一映射．但

$$a^h a^k=a^{h+k}\longrightarrow h+k$$

所以 $$G\cong\bar{G}$$

第二种情形：a 的阶是 n，$a^n=e$。这时

$$a^h=a^k,\text{ 当而且只当 } n\mid h-k \text{ 的时候.}$$

假如 $n\mid h-k$，那么 $h-k=nq$，$h=k+nq$，

$$a^h=a^{k+nq}=a^ka^{nq}=a^k(a^n)^q=a^ke^q=a^k$$

假如 $a^h=a^k$，叫 $h-k=nq+r$，$0\leqslant r\leqslant n-1$，那么

$$e=a^{h-k}=a^{nq+r}=a^{nq}a^r=ea^r=a^r$$

由阶的定义，$r=0$，也就是说，$n\mid h-k$。

这样，

$$a^k\longrightarrow[k]$$

是 G 与剩余类加群 $\bar{G}$ 间的一一映射．但

$$a^ha^k=a^{h+k}\longrightarrow[h+k]=[h]+[k]$$

所以 $$G\cong\bar{G}$$ 证完

让我们看一看，到现在为止我们对于循环群已经知道了些什么．假如有一个循环群，这个群一定有一个生成元，这个元一定有一个固定的阶．这个阶或是无限大，或是一个正整数 n．由于例 1 和例 2，我们知道，生成元的阶是无限大或是一个给定的正整数 n 的循环群是有的．由定理，我们知道，抽象地来看，生成元的阶是无限大的循环群只有一个，生成元的阶是给定的正整数 n 的循环群也只有一个．至于这些循环群的构造，我们也知道得很清楚：

假如 $G=(a)$，a 的阶是无限大，那么

G 的元是 $\cdots,a^{-2},a^{-1},a^0,a^1,a^2,\cdots$

G 的乘法是 $a^ha^k=a^{h+k}$

假如 $G=(a)$，a 的阶是 n，那么

G 的元可以写成 $a^0,a^1,a^2,\cdots,a^{n-1}$

G 的乘法是 $a^ia^k=a^{r_{ik}}$

这里 $i+k=nq+r_{ik}$，$0\leqslant r_{ik}\leqslant n-1$

这样，我们对于循环群的存在问题，数量问题，构造问题都已能解答，循环群已完全在我们的掌握之中．这一节的研讨是近世代数的研讨的一个缩影．在近世代数里，不管是在群论里还是在其它部门里，我们研究一种代数系统就是要解决这一种系统的存在问题，数量问题和构造问题．假如我们对于这三个问题能得到如同我们对于循环群所得到的这样完满的解答，我们的目的就算达到了。

习　题

1．证明，一个循环群一定是交换群．

2．假定群的元 a 的阶是 n，证明 a^r 的阶是 $\frac{n}{d}$，这里 $d=(r,\ n)$ 是 r 和 n 的最大公因子．

3．假定 a 生成一个阶是 n 的循环群 G．证明：a^r 也生成 G，假如 $(r,\ n)=1$（这就是说 r 和 n 互素）．

4．假定 G 是循环群，并且 G 与 $\bar{G}$ 同态．证明 $\bar{G}$ 也是循环群．

5．假定 G 是无限阶的循环群，$\bar{G}$ 是任何循环群．证明 G 与 $\bar{G}$ 同态．

§8．子　　群

在群论里像循环群那样完全解决了的群只有很少的几种．对于其余的几种我们为篇幅所限，不能一一加以讨论．我们以下要介绍几种研究任何群都要用到的一般方法．这些方法都是利用一个群的子集来推测整个群的性质。

我们看一个群 G．假如由 G 里取出一个子集 H 来，那么利用 G 的乘法可以把 H 的两个元相乘．对于这个乘法来说，H 很可能也作成一个群．

定义　一个群 G 的一个子集 H 叫做 G 的一个**子群**，假如 H 对于 G 的乘法来说作成一个群。

例 1 给了一个任意群 G, G 至少有两个子群:

1. G;

2. 只包含单位元 e 的子集.

例 2 $G=S_3$, $H=\{(1),(12)\}$. 那么 H 是 S_3 的一个子群. 因为:

Ⅰ. H 对于 G 的乘法来说是闭的,

$$(1)(1)=(1),\ (1)(12)=(12),$$

$$(12)(1)=(12),\ (12)(12)=(1);$$

Ⅱ. 结合律对于所有 G 的元都对, 对于 H 的元也对;

Ⅳ. $(1)\in H$;

Ⅴ. $(1)(1)=(1)$, $(12)(12)=(1)$.

现在让我们看一看, 一个子集 H 作成一个子群的条件是什么. 要知道 H 是不是作成一个子群, 我们用不着像例 2 那样, 看 H 是不是适合群定义的全部条件. 我们有

定理 1 一个群 G 的一个不空子集 H 作成 G 的一个子群的充分而且必要条件是:

(i) $a, b\in H \Longrightarrow ab\in H$

(ii) $a\in H \Longrightarrow a^{-1}\in H$

证明 若是(i), (ii)成立, H 作成一个群.

Ⅰ. 由于(i), H 是闭的;

Ⅱ. 结合律在 G 中成立, 在 H 中自然成立;

Ⅳ. 因为 H 至少有一个元 a, 由(ii), H 也有元 a^{-1}, 所以由(i),

$$a^{-1}a=e\in H$$

Ⅴ. 由(ii), 对于 H 的任意元 a 来说, H 有元 a^{-1}, 使得

$$a^{-1}a=e$$

反过来看, 假如 H 是一个子群, (i)显然成立. 我们证明, 这时(ii)也一定成立. H 既是一个群, H 一定有一个单位元 e'. 我们

在H里任意取一个元a，就得到$e'a=a$．但e'和a都属于G，所以e'是方程$ya=a$在G里的一个解．但这个方程在G里只有一个解，就是G的单位元e．所以

$$e'=e\in H$$

这样，因为H是一个群，方程$ya=e$在H中有解a'，但a'也是这个方程在G里的解，而这个方程在G里只有一个解，就是a^{-1}．所以

$$a'=a^{-1}\in H$$

证完

推论 假定H是群G的一个子群．那么H的单位元就是G的单位元，H的任意元a在H里的逆元就是a在G里的逆元．

(i)，(ii)两个条件也可以用一个条件来代替．

定理2 一个群G的一个不空子集H作成G的一个子群的充分而且必要条件是：

(iii) $a, b\in H \Longrightarrow ab^{-1}\in H$

证明 我们先证明，(i)和(ii)成立，(iii)就也成立．假定a, b属于H，由(ii)，$b^{-1}\in H$，由(i)，

$$ab^{-1}\in H$$

现在我们反过来证明，由(iii)可以得到(i)和(ii)．假定$a\in H$．由(iii)，$aa^{-1}=e\in H$，于是

$$ea^{-1}=a^{-1}\in H$$

假定$a\in H, b\in H$．由刚证明的，$b^{-1}\in H$；由(iii)，

$$a(b^{-1})^{-1}=ab\in H$$

证完

假如所给子集H是一个有限集合，那么H作成子群的条件更要简单．

定理3 一个群G的一个不空有限子集H作成G的一个子群的充分而且必要条件是：

$$a, b\in H \Longrightarrow ab\in H$$

证明 这个条件是必要的，无须证明．我们证明它是充分的．

因为H是有限集合，我们只须证明，若是H适合以上条件，H就适合群定义的条件 I, II, III'. 但这是非常明显的，因为 I 就是给的条件，II, III' 在G里是对的，在H里也一定对. 证完.

现在我们要认识一种找一个子群的一般方法.

我们在一个群G里任意取出一个不空子集S来，S包含元a, b, c, d, …. 那么S当然不见得是一个子群. 但是我们可以把S扩大一点，而得到一个包含S的子群.

利用S的元以及这些元的逆元我们可以作各种乘积，比方说，

$$ab, \quad a^{-2}c, \quad b^3cb^{-1}, \quad d, \quad c^{-1}$$

等等. 我们作一个集合H，让它刚好包含所有这样的乘积. 因为两个这样的乘积乘起来还是一个这样的乘积，一个这样的乘积的逆元也是一个这样的乘积，由定理 1, H 作成一个子群.

H显然包含S. 包含S的子群一般不止一个，比方说，G就是这样的一个. 但一个包含S的子群H'一定包含H. 这一点容易看出：H'既是一个子群，必须适合(i), (ii)两个条件，因而，由于它包含所有S的元a, b, c, …，它必须包含所有的上面所作的那些乘积；这就是说，$H' \supset H$. 这样看起来，H是包含S的最小的子群.

定义 如上得到的H叫做由S生成的子群，我们用符号(S)来表示它.

假如我们取一个只包含一个元a的子集S，那么

$$(S)=(a)$$

是一个循环子群.

习 题

1. 找出S_3的所有子群.
2. 证明，群G的两个子群的交集也是G的子群.
3. 取S_3的子集$S=\{(12), (123)\}$. S生成的子群包含哪些个元？一个

群的两个不同的子集会不会生成相同的子群？

4．证明，循环群的子群也是循环群．

5．找出模12的剩余类加群的所有子群．

6．假定H是群G的一个非空子集，并且H的每一个元的阶都有限．证明，H作成子群的充要条件是：

$$a,\ b\in H \Longrightarrow ab\in H$$

§9．子群的陪集

在这一节里我们要利用群G的一个子群H来作一个G的分类，然后由这个分类推出几个重要的定理．

我们曾经利用一个整数n把全体整数分成剩余类．让我们把这种分类法从另一个观点来考察一下．我们把整数加群叫做$\bar{G}$，把包含所有n的倍数的集合叫做$\bar{H}$，

$$\bar{H}=\{hn\},\quad (h=\cdots,-2,-1,0,1,2,\cdots)$$

那么对于$\bar{H}$的任意两个元hn同kn来说，

$$hn+(-kn)=(h-k)n\in\bar{H}$$

但$-kn$是kn在$\bar{G}$里的逆元，$+$是$\bar{G}$的代数运算，由Ⅱ，8，定理2，$\bar{H}$是$\bar{G}$的一个子群．

我们把$\bar{G}$分成剩余类时所利用的等价关系是如下规定的：

$$a\equiv b\ (n),\quad \text{当而且只当}\ n\mid a-b\ \text{的时候}$$

但$n\mid a-b$就是说$a-b=kn$，也就是说$a-b\in\bar{H}$；反过来说，如果$a-b\in\bar{H}$，也就有$n\mid a-b$．所以上述等价关系也可以如下规定：

$$a\equiv b\ (n),\quad \text{当而且只当}\ a-b\in\bar{H}\ \text{的时候}$$

这样，我们也可以说$\bar{G}$的剩余类是利用子群$\bar{H}$来分的．利用一个子群H来把一个群G分类，正是以上特殊情形的推广．

我们看一个群G和G的一个子群H．我们规定一个G的元中间的关系～：

$$a \sim b，\text{当而且只当} ab^{-1} \in H \text{的时候}$$

给了 a 和 b，我们可以唯一决定，ab^{-1} 是不是属于 H，所以～是一个关系．但

Ⅰ．$aa^{-1} = e \in H$．所以

$$a \sim a$$

Ⅱ．$ab^{-1} \in H \Longrightarrow (ab^{-1})^{-1} = ba^{-1} \in H$，所以

$$a \sim b \Longrightarrow b \sim a$$

Ⅲ．$ab^{-1} \in H$，$bc^{-1} \in H \Longrightarrow (ab^{-1})(bc^{-1}) = ac^{-1} \in H$，所以

$$a \sim b,\ b \sim c \Longrightarrow a \sim c$$

这样，～是一个等价关系．利用这个等价关系，我们可以得到一个 G 的分类．这样得来的类有一个特殊的名字，并且用一种特殊的符号来表示它们．

定义 由上面的等价关系～所决定的类叫做子群 H 的**右陪集**．包含元 a 的右陪集用符号 Ha 来表示．

我们所以用这个名词和这种符号是由于以下的事实：假如我们用 a 从右边去乘 H 的每一个元，就得到了包含 a 的类，这就是说，Ha 刚好包含所有可以写成

$$ha \qquad (h \in H)$$

形式的 G 的元．

这个事实很容易证明．假定

$$b \in Ha$$

那么 $b \sim a$．也就是说，$ba^{-1} = h \in H$．这样

$$b = ha \qquad (h \in H)$$

反过来说，假定

$$b = ha$$

那么 $ba^{-1} = h \in H$．也就是说，$b \sim a$．这样

$$b \in Ha$$

例1 $G=S_3=\{(1),(12),(13),(23),(123),(132)\}$

$$H=\{(1),(12)\}$$

那么

$$H(1)=\{(1),(12)\}$$

$$H(13)=\{(13),(123)\}$$

$$H(23)=\{(23),(132)\}$$

我们还可以用(12),(123),(132)来作右陪集

$$H(12),\ H(123),\ H(132)$$

但因为

$$(12)\in H(1),\ (123)\in H(13),\ (132)\in H(23)$$

所以一定有

$$H(12)=H(1),\ H(123)=H(13),\ H(132)=H(23)$$

我们算一个来测验一下：

$$H(123)=\{(123),\ (13)\}$$

$$H(123)=H(13)$$

这样，子群H把整个群G分成$H(1)$，$H(13)$，$H(23)$三个不同的右陪集. 这三个右陪集放在一起显然正是G，因此，它们的确是G的一个分类.

右陪集是从等价关系～：

$$a\sim b,\ \text{当而且只当}\ ab^{-1}\in H\ \text{的时候}$$

出发而得到的. 假如我们规定一个关系～′：

$$a\sim' b,\ \text{当而且只当}\ b^{-1}a\in H\ \text{的时候}$$

那么同以上一样可以看出，～′也是一个等价关系. 利用这个等价关系，我们可以得到G的另一个分类.

定义 由等价关系～′所决定的类叫作子群H的**左陪集**. 包含元a的左陪集我们用符号aH来表示.

同以上一样我们可以证明：aH刚好包含所有可以写成

$$ah \qquad (h \in H)$$

形式的 G 的元.

因为一个群的乘法不一定适合交换律，所以一般来说，$\sim$ 和 $\sim'$ 两个关系并不相同，H 的右陪集和左陪集也就不相同.

例 2 例 1 里的 H 的左陪集是

$(1)H=\{(1),(12)\}$

$(13)H=\{(13),(132)\}$

$(23)H=\{(23),(123)\}$

这和 H 的右陪集并不相同.

但是一个子群的左右陪集之间有一个共同点.

定理 1 一个子群 H 的右陪集的个数和左陪集的个数相等：它们或者都是无限大，或者都有限并且相等.

证明 我们把 H 的右陪集所作成的集合叫做 S_r，H 的左陪集所作成的集合叫做 S_l. 我们说，

$$\phi: \qquad Ha \longrightarrow a^{-1}H$$

是一个 S_r 与 S_l 间的一一映射. 因为：

(i) $Ha=Hb \Longrightarrow ab^{-1}\in H \Longrightarrow (ab^{-1})^{-1}=ba^{-1}\in H$

$\Longrightarrow a^{-1}H=b^{-1}H$

所以右陪集 Ha 的象与 a 的选择无关，ϕ 是一个 S_r 到 S_l 的映射；

(ii) S_l 的任意元 aH 是 S_r 的元 Ha^{-1} 的象，所以 ϕ 是一个满射；

(iii) $Ha\neq Hb \Longrightarrow ab^{-1}\bar{\in} H \Longrightarrow (ab^{-1})^{-1}=ba^{-1}\bar{\in} H$

$\Longrightarrow a^{-1}H\neq b^{-1}H$

S_r 与 S_l 间既有一一映射存在，定理显然是对的. 证完.

定义 一个群 G 的一个子群 H 的右陪集（或左陪集）的个数叫做 H 在 G 里的**指数**.

下面我们要用右陪集来证明几个重要定理. 因为左陪集和右

陪集的对称性，凡是我们以下用右陪集的地方也都可以用左陪集来代替.

引理 一个子群H与H的每一个右陪集Ha之间都存在一个一一映射.

证明 ϕ: $$h \longrightarrow ha$$
是H与Ha间的一一映射. 因为:

(i) H的每一个元h有一个唯一的象ha;

(ii) Ha的每一个元ha是H的h的象;

(iii) 假如$h_1a=h_2a$, 那么$h_1=h_2$. 证完.

由这个引理，我们可以得到极重要的定理2和定理3.

定理 2 假定H是一个有限群G的一个子群. 那么H的阶n和它在G里的指数j都能整除G的阶N，并且
$$N=nj$$

证明 G的阶N既是有限，H的阶n和指数j也都是有限正整数. G的N个元被分成j个右陪集，而且由引理，每一个右陪集都有n个元，所以
$$N=nj$$
证完

定理 3 一个有限群G的任一个元a的阶n都整除G的阶.

证明 a生成一个阶是n的子群，由以上定理，n整除G的阶. 证完.

例 3 我们还是看例1的S_3同$H=\{(1),(12)\}$.

S_3的阶是6; H的阶是2; H有三个右陪集，H的指数是3. 2和3果然整除6，并且
$$6=2\times3$$

S_3的六个元是(1), (12), (23), (13), (123), (132). 它们的阶是1或2或3. 1,2,3都整除6.

习　　题

1. 证明，阶是素数的群一定是循环群.

2. 证明，阶是 p^m 的群（p 是素数）一定包含一个阶是 p 的子群.

3. 假定 a 和 b 是一个群 G 的两个元，并且 $ab=ba$. 又假定 a 的阶是 m，b 的阶是 n，并且 $(m,n)=1$. 证明：ab 的阶是 mn.

4.* 假定～是一个群 G 的元间的一个等价关系，并且对于 G 的任意三个元 a, x, x' 来说，

$$ax \sim ax' \Longrightarrow x \sim x'$$

证明，与 G 的单位元 e 等价的元所作成的集合是 G 的一个子群.

5. 我们直接下右陪集 Ha 的定义如下：Ha 刚好包含 G 的可以写成

$$ha \qquad (h \in H)$$

形式的元. 由这个定义推出以下事实：G 的每一个元属于而且只属于一个右陪集.

6.* 若我们把同构的群看作一样的，一共只存在两个阶是 4 的群. 它们都是交换群.

§10. 不变子群、商群

我们在这一节里要讲到一种最重要的子群，就是**不变子群**.

给了一个群 G，一个子群 H，那么 H 的一个右陪集 Ha 未必等于 H 的左陪集 aH，这一点我们在上一节的例 2 里已经看到.

定义　一个群 G 的一个子群 N 叫做一个**不变子群**，假如对于 G 的每一个元 a 来说，都有

$$Na=aN$$

一个不变子群 N 的一个左（或右）陪集叫做 N 的一个**陪集**.

例 1　一个任意群 G 的子群 G 和 e 总是不变子群，因为对于任意 G 的元 a 来说，

$$Ga=aG=G.$$

$$ea=ae=a$$

例 2　N刚好包含群G的所有有以下性质的元n，

$$na=an,\ \text{不管}\ a\ \text{是}\ G\ \text{的哪一个元}$$

那么N是G的一个不变子群．因为$N\ni e$，所以N是非空的．又

$$n_1a=an_1,\ n_2a=an_2\Longrightarrow n_1n_2a=n_1an_2=an_1n_2$$

$$na=an\Longrightarrow n^{-1}a=n^{-1}ann^{-1}=n^{-1}nan^{-1}=an^{-1}$$

这就是说，

$$n_1\in N,\ n_2\in N\Longrightarrow n_1n_2\in N;\quad n\in N\Longrightarrow n^{-1}\in N$$

由Ⅱ,8，定理1，N是一个子群．但G的每一个元a可以同N的每一个元n交换，所以我们显然有$Na=aN$，即N是不变子群．

这个不变子群叫做G的中心．

例 3　一个交换群G的每一个子群H都是不变子群．因为G的每一个元a可以和任意一元x交换，$xa=ax$，所以对于一个子群H来说，自然也有

$$Ha=aH$$

例 4　$G=S_3$．那么

$$N=\{(1),\ (123),\ (132)\}$$

是一个不变子群．N是子群容易看出，因为$N=((123))$．但

$$N(1)=\{(1),(123),(132)\},(1)N=\{(1),(123),(132)\}$$

$$N(12)=\{(12),(23),(13)\},(12)N=\{(12),(13),(23)\}$$

所以　$N(1)=N(123)=N(132)=(1)N=(123)N=(132)N$

$$N(12)=N(23)=N(13)=(12)N=(23)N=(13)N$$

有一点我们应该注意，所谓$aN=Na$，并不是说a可以同N的每一个元交换，而是说aN和Na这两个集合一样(参看例4)．

现在我们看一看，一个子群作成不变子群的其它几个条件．我们先规定一个符号．

定义　假定$S_1,S_2,\cdots,S_m$是一个群G的m个子集．那么由所

有可以写成

$$s_1s_2\cdots s_m \qquad (s_i\in S_i)$$

形式的G的元作成的集合叫做$S_1, S_2, \cdots, S_m$的乘积. 这个乘积我们用符号

$$S_1S_2\cdots S_m$$

来表示.

我们很容易看出:

$$S_1(S_2S_3)=(S_1S_2)S_3$$

定理 1 一个群G的一个子群N是一个不变子群的充分而且必要条件是:

$$aNa^{-1}=N$$

对于G的任意一个元a都对.

证明 假如N是不变子群,那么对于G的任何a来说,

$$aN=Na$$

这样,

$$aNa^{-1}=(aN)a^{-1}=(Na)a^{-1}=N(aa^{-1})=Ne=N$$

假如对于G的任何a来说,

$$aNa^{-1}=N$$

那么

$$Na=(aNa^{-1})a=(aN)(a^{-1}a)=(aN)e=aN$$

N是不变子群. 证完.

定理 2 一个群G的一个子群N是一个不变子群的充分而且必要条件是:

$$a\in G,\ n\in N\Longrightarrow ana^{-1}\in N$$

证明 这个条件是必要的，是定理1的直接结果. 我们证明它也是充分的. 假定这个条件成立，那么对于G的任何一个元a来说

(1) $$aNa^{-1}\subset N$$

这样，因为 a^{-1} 也是 G 的元，我们有

$$a^{-1}Na\subset N,\ a(a^{-1}Na)a^{-1}\subset aNa^{-1}$$

(2) $$N\subset aNa^{-1}$$

由(1)和(2) $$aNa^{-1}=N$$

因而由定理 1，N 是不变子群．证完．

要测验一个子群是不是不变子群，用定理 2 的条件一般比较方便．

不变子群所以重要，是因为这种子群的陪集，对于某种与原来的群有密切关系的代数运算来说，也作成一个群．

我们再回过去看一看整数加群 $\bar{G}$．我们知道，一个固定整数 n 的所有倍数作成一个子群（Ⅱ，9）．这个子群我们现在把它叫做 $\bar{N}$．因为 $\bar{G}$ 是交换群，$\bar{N}$ 是一个不变子群．我们也知道，$\bar{N}$ 的陪集，也就是模 n 的剩余类，对于代数运算

$+$： $$[a]+[b]=[a+b]$$

来说，作成一个群：剩余类加群(Ⅱ，7，例 2)．

把一个任意不变子群的陪集作成一个群的方法正是以上特例的推广．

我们看一个群 G 的一个不变子群 N．把 N 的所有陪集作成一个集合

$$S=\{aN,bN,cN,\cdots\}$$

我们说，法则

$$(xN)(yN)=(xy)N$$

是一个 S 的乘法．要看清这一点，我们只须证明，两个陪集 xN 和 yN 的乘积与代表 x 和 y 的选择无关．让我们看一看：

假定 $$xN=x'N,\ yN=y'N$$

那么 $$x=x'n_1,\ y=y'n_2,\ (n_1,\ n_2\in N)$$

$$xy=x'n_1y'n_2$$

但由于N是不变子群，

$$n_1y'\in Ny'=y'N$$

所以

$$n_1y'=y'n_3 \qquad (n_3\in N)$$

$$xy=x'y'(n_3n_2)$$

$$xy\in x'y'N$$

由此我们果然有

$$xyN=x'y'N$$

定理 3　一个不变子群的陪集对于上边规定的乘法来说作成一个群.

证明　我们证明群定义的条件 I, II, IV, V 能被满足.

I. 显然，

II.
$$(xNyN)zN=[(xy)N]zN=(xyz)N$$
$$xN(yNzN)=xN[(yz)N]=(xyz)N$$

IV.
$$eNxN=(ex)N=xN$$

V.
$$x^{-1}NxN=(x^{-1}x)N=eN$$

证完

定义　一个群G的一个不变子群N的陪集所作成的群叫做一个**商群**. 这个群我们用符号G/N来表示.

因为N的指数就是N的陪集的个数，我们显然有，**商群G/N的元的个数等于N的指数**. 当G是有限群的时候，由 II, 9, 定理 2,

$$\frac{G\text{ 的阶}}{N\text{ 的阶}}=G/N\text{ 的阶}$$

习　　题

1. 假定群G的不变子群N的阶是 2. 证明，G的中心包含N.
2. 证明，两个不变子群的交集还是不变子群.
3. 证明，指数是 2 的子群一定是不变子群.
4. 假定H是G的子群，N是G的不变子群. 证明，HN是G的子群.

5. 举例证明，G的不变子群N的不变子群N_1未必是G的不变子群（取$G=S_4$）.

6.* 一个群G的可以写成$a^{-1}b^{-1}ab$形式的元叫做换位子. 证明：

(i) 所有的有限个换位子的乘积作成的集合C是G的一个不变子群；

(ii) G/C是交换群；

(iii) 若N是G的一个不变子群，并且G/N是交换群，那么

$$N\supset C$$

§11. 同态与不变子群

在不变子群，商群与同态映射之间存在几个极端重要的关系. 知道了这几个关系，我们才能看出不变子群和商群的重要意义.

首先我们有

定理 1 一个群G同它的每一个商群G/N同态.

证明 我们规定一个法则

$$a\longrightarrow aN \qquad (a\in G)$$

这显然是G到G/N的一个满射. 对于G的任意两个元a和b来说，

$$ab\longrightarrow abN=(aN)(bN)$$

所以它是一个同态满射. 证完.

由群G的一个子群可以推测整个群G的性质，我们在Ⅱ，9已经看到了一点. 假如我们有一个不变子群N，由Ⅱ,10，我们知道，就同时有两个群可以供我们利用，一个是N本身，另一个是商群G/N. 现在定理1又告诉我们，G与G/N同态，这样我们自然更容易推测G的性质.

不变子群的重要性不仅在这一方面，因为在某种意义之下，定理1的逆定理也是对的. 我们先规定一个名词.

定义 假定ϕ是一个群G到另一个群$\bar{G}$的一个同态满射. $\bar{G}$

的单位元 $\bar{e}$ 在 ϕ 之下的所有逆象所作成的 G 的子集叫做同态满射 ϕ 的核.

定理 2 假定 G 和 $\bar{G}$ 是两个群,并且 G 与 $\bar{G}$ 同态,那么这个同态满射的核 N 是 G 的一个不变子群,并且

$$G/N \cong \bar{G}$$

证明 我们用 ϕ 来表示给的同态满射. 假定 a 和 b 是 N 的任何两个元,那么在 ϕ 之下,

$$a \longrightarrow \bar{e}, \quad b \longrightarrow \bar{e}$$

因此 $$ab^{-1} \longrightarrow \bar{e}\bar{e}^{-1} = \bar{e}$$

这就是说, $$a, b \in N \Longrightarrow ab^{-1} \in N$$

N 是 G 的一个子群. 假定 $n \in N$, $a \in G$, 而且在 ϕ 之下, $a \longrightarrow \bar{a}$. 那么在 ϕ 之下,

$$a \longrightarrow \bar{a}, \quad n \longrightarrow \bar{e}$$

$$ana^{-1} \longrightarrow \bar{a}\bar{e}\bar{a}^{-1} = \bar{e}$$

这就是说, $$n \in N, \quad a \in G \Longrightarrow ana^{-1} \in N$$

N 是 G 的一个不变子群.

现在规定一个法则

ψ: $$aN \longrightarrow \bar{a} = \phi(a) \qquad (a \in G)$$

我们说,这是一个 G/N 与 $\bar{G}$ 间的同构映射. 因为:

(i) $aN = bN \Longrightarrow b^{-1}a \in N \Longrightarrow \bar{b}^{-1}\bar{a} = \bar{e} \Longrightarrow \bar{a} = \bar{b}$,

这就是说,在 ψ 之下 G/N 的一个元素只有一个唯一的象;

(ii) 给了 $\bar{G}$ 的一个任意元 $\bar{a}$, 在 G 里至少有一个元 a 满足条件 $\phi(a) = \bar{a}$, 由 ψ 的定义,

ψ: $$aN \longrightarrow \text{给的 } \bar{a}$$

这就是说, ψ 是 G/N 到 $\bar{G}$ 的满射;

(iii) $aN \neq bN \Longrightarrow b^{-1}a \bar{\in} N \Longrightarrow \bar{b}^{-1}\bar{a} \neq \bar{e} \Longrightarrow \bar{a} \neq \bar{b}$

(iv) 在 ψ 之下,

$$aNbN = abN \longrightarrow \overline{ab} = \bar{a}\bar{b}$$

这样 $G/N \cong \bar{G}$ 证完

定理 1 告诉我们，一个群 G 和它的每一个商群同态，定理 2 告诉我们，抽象地来看，G 只能和它的商群同态，所以我们可以说，定理 2 正是定理 1 的反面．我们知道，当群 G 与群 $\bar{G}$ 同态的时候，$\bar{G}$ 的性质并不同 G 的完全一样．但定理 2 告诉我们，这时我们一定找得到 G 的一个不变子群 N，使得 $\bar{G}$ 的性质和商群 G/N 的完全一样．从这里我们可以看出，不变子群和商群的重要意义．

群的同态满射的核是一个不变子群，这一件重要事实是一个一般事实的特例．我们知道，在一个同态满射之下，一个群的若干性质是不变的，若干性质是会变的．让我们看一看，同态满射对于子群和不变子群所发生的影响如何．为说明方便起见，我们先规定子集的象与逆象这两个概念．

定义 假定 ϕ 是集合 A 到集合 $\bar{A}$ 的一个满射．

我们说，$\bar{S}$ 是 A 的一个子集 S 在 ϕ 之下的象，假如 $\bar{S}$ 刚好包含所有 S 的元在 ϕ 之下的象．

我们说，S 是 $\bar{A}$ 的一个子集 $\bar{S}$ 在 ϕ 之下的逆象，假如 S 刚好包含所有 $\bar{S}$ 的元在 ϕ 之下的逆象．

定理 3 假定 G 和 $\bar{G}$ 是两个群，并且 G 与 $\bar{G}$ 同态．那么在这个同态满射之下的

（i） G 的一个子群 H 的象 $\bar{H}$ 是 $\bar{G}$ 的一个子群；

（ii） G 的一个不变子群 N 的象 $\bar{N}$ 是 $\bar{G}$ 的一个不变子群．

证明 我们用 ϕ 来表示给定的同态满射．

（i） 假定 $\bar{a}, \bar{b}$ 是 $\bar{H}$ 的两个任意元，并且在 ϕ 之下，

$$a \longrightarrow \bar{a}, \quad b \longrightarrow \bar{b} \quad (a, b \in H)$$

那么在 ϕ 之下，

$$ab^{-1} \longrightarrow \bar{a}\bar{b}^{-1}$$

但由于H是子群，$ab^{-1}\in H$，因此由于$\bar{H}$是H的在ϕ之下的象，$\bar{a}\bar{b}^{-1}\in\bar{H}$. 这样，

$$\bar{a},\bar{b}\in\bar{H}\Longrightarrow\bar{a}\bar{b}^{-1}\in\bar{H}$$

$\bar{H}$是$\bar{G}$的一个子群.

(ii) N既是G的一个不变子群，由(i)，我们知道$\bar{N}$是$\bar{G}$的一个子群. 假定$\bar{a}$是$\bar{G}$的任意元，$\bar{n}$是$\bar{N}$的任意元，而且在ϕ之下，

$$a\longrightarrow\bar{a},\quad n\longrightarrow\bar{n}\quad(a\in G, n\in N)$$

那么在ϕ之下，

$$ana^{-1}\longrightarrow\bar{a}\bar{n}\bar{a}^{-1}$$

但由于N是G的不变子群，$ana^{-1}\in N$，因此由于$\bar{N}$是N在ϕ之下的象，$\bar{a}\bar{n}\bar{a}^{-1}\in\bar{N}$. 这样，

$$\bar{a}\in\bar{G},\bar{n}\in\bar{N}\Longrightarrow\bar{a}\bar{n}\bar{a}^{-1}\in\bar{N}$$

$\bar{N}$是$\bar{G}$的一个不变子群. 证完.

定理 4 假定G和$\bar{G}$是两个群，并且G与$\bar{G}$同态. 那么在这个同态满射之下的

(i) $\bar{G}$的一个子群$\bar{H}$的逆象H是G的一个子群；

(ii) $\bar{G}$的一个不变子群$\bar{N}$的逆象N是G的一个不变子群.

证明 我们用ϕ来表示给定的同态满射.

(i) 假定a,b是H的两个任意元，并且在ϕ之下，

$$a\longrightarrow\bar{a},\quad b\longrightarrow\bar{b}$$

那么由于H是$\bar{H}$的逆象，$\bar{a},\bar{b}\in\bar{H}$，因而$\bar{a}\bar{b}^{-1}\in\bar{H}$. 但在$\phi$之下，

$$ab^{-1}\longrightarrow\bar{a}\bar{b}^{-1}$$

所以$ab^{-1}\in H$. 这样，

$$a,b\in H\Longrightarrow ab^{-1}\in H$$

H是G的一个子群.

(ii) $\bar{N}$既是$\bar{G}$的一个不变子群，由(i)，我们知道N是G的一个子群. 假定a是G的任意元，n是N的任意元，并且在ϕ

之下，

$$a \longrightarrow \bar{a}, \quad n \longrightarrow \bar{n}$$

那么 $\bar{a} \in \bar{G}$，$\bar{n} \in \bar{N}$，因而由于 $\bar{N}$ 是不变子群，$\bar{a}\bar{n}\bar{a}^{-1} \in \bar{N}$．但在 ϕ 之下，

$$ana^{-1} \longrightarrow \bar{a}\bar{n}\bar{a}^{-1}$$

所以 $ana^{-1} \in N$．这样，

$$a \in G, n \in N \Longrightarrow ana^{-1} \in N$$

N 是 G 的一个不变子群．证完．

这样，一个群的一个子集是否一个子群以及是否一个不变子群这两个性质，在一个同态满射之下是不变的．这一点更增加了子群以及不变子群的重要性．

同态满射的核是不变子群，这一件事实显然是定理 4，(ii)的一个特例．

习　题

1．我们看一个集合 A 到集合 $\bar{A}$ 的满射 ϕ．证明，若 S 是 $\bar{S}$ 的逆象，$\bar{S}$ 一定是 S 的象；但若 $\bar{S}$ 是 S 的象，S 不一定是 $\bar{S}$ 的逆象．

2．假定群 G 与群 $\bar{G}$ 同态，$\bar{N}$ 是 $\bar{G}$ 的一个不变子群，N 是 $\bar{N}$ 的逆象．证明，$G/N \cong \bar{G}/\bar{N}$．

3．假定 G 和 $\bar{G}$ 是两个有限循环群，它们的阶各是 m 和 n．证明，G 与 $\bar{G}$ 同态，当而且只当 $n|m$ 的时候．

4．假定 G 是一个循环群，N 是 G 的一个子群．证明，G/N 也是循环群．

第三章　环与域

在前一章里我们把群的基本性质稍为讨论了一下. 现在我们要谈到其它两种代数系统，就是环与域. 在高等代数里我们已经看到，全体整数作成一个环，全体有理数，全体实数或全体复数都作成一个域. 即此可见，环与域这两个概念的重要性. 同我们对于群的讨论一样，在这一章里，我们只是要讨论环与域的若干最基本的性质，并且认识几种最重要的环与域，使得我们一方面对于中学代数有更清楚的了解，另一方面得到作进一步研讨的基本知识.

§1. 加群、环的定义

在环的定义里要用到加群这一个概念. 我们先把这个概念说明一下. 抽象群的代数运算到现在为止我们都用乘法的符号来表示. 但我们知道，一个代数运算用什么符号来表示是没有关系的. 一个交换群的代数运算，在某种场合之下，用加法的符号来表示更为方便.

定义　一个交换群叫做一个**加群**，假如我们把这个群的代数运算叫做加法，并且用符号＋来表示.

群论里的许多符号都是因为把群的代数运算叫做了乘法才那样选择的. 因此在加群里我们有选择新符号的必要. 符号一改变，许多计算规则的形式当然也跟着改变. 现在我们简单地说明一下加群的符号和计算规则.

由于加群的加法适合结合律，n 个元 a_1, a_2, …, a_n 的和有意义，这个和我们有时用符号 $\sum_{i=1}^{n} a_i$ 来表示：

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$$

一个加群的唯一的单位元我们用 0 来表示，并且把它叫做零元．我们有以下计算规则：

(1) $$0+a=a+0=a \qquad (a\text{ 是任意元})$$

元 a 的唯一的逆元我们用 $-a$ 来表示，并且把它叫做 a 的负元(简称负 a)．元 $a+(-b)$我们简写成 $a-b$ (念成 a 减 b)．由这两个定义以及交换群的性质，我们有以下计算规则：

(2) $$-a+a=a-a=0$$

(3) $$-(-a)=a$$

(4) $$a+c=b \Longleftrightarrow c=b-a$$

(5) $$-(a+b)=-a-b, \quad -(a-b)=-a+b$$

比方说要证明(5)的第一式，照 $-(a+b)$的定义，只须证明

$$(-a-b)+(a+b)=0$$

而事实上，

$$(-a-b)+(a+b)=-a+(-b)+a+b=0$$

n 个 a 的和(n 是正整数)我们用符号 na 来表示，并且把它叫做 a 的 n 倍(简称 n 倍 a)：

$$na=\overbrace{a+a+\cdots+a}^{n\text{ 个}}$$

正如乘法群的情形一样，我们进一步规定：

$$(-n)a=-(na), \quad 0a=0$$

这里第一个 0 是整数零，第二个 0 是加群的零元．这一点初看似乎很混乱，但正如用同一符号来表示两种不同的代数运算的情形一样，习惯了就不觉得有什么不便了．这样规定以后，对于任何整数 m, n 和加群的任何元 a, b 来说，都有

$$ma+na=(m+n)a$$

(6) $$m\cdot na = mn\cdot a$$

$$n(a+b) = na+nb$$

这几个公式与乘法群的相当公式完全平行. 我们要注意，这里的整数 m, n 一般不是加群的元.

用新的符号，加群的一个非空子集 S 作成一个子群的充分必要条件是：

$$a, b\in S \Longrightarrow a+b\in S$$

$$a\in S \Longrightarrow -a\in S$$

或是

$$a, b\in S \Longrightarrow a-b\in S$$

现在让我们看一看，什么叫做一个环.

定义 一个集合 R 叫做一个环，假如

1. R 是一个加群，换一句话说，R 对于一个叫做加法的代数运算来说作成一个交换群；

2. R 对于另一个叫做乘法的代数运算来说是闭的；

3. 这个乘法适合结合律：

$$a(bc) = (ab)c$$

不管 a, b, c 是 R 的哪三个元；

4. 两个分配律都成立：

$$a(b+c) = ab+ac$$

$$(b+c)a = ba+ca$$

不管 a, b, c 是 R 的哪三个元.

由高等代数已知，全体整数作成的集合对于普通加法和乘法来说作成一个环.

在没有举别的例以前，让我们先看一看，在一个环里有些什么计算规则.

因为一个环是一个加群，上面的计算规则(1)到(6)在一个环

里都成立.

由于两个分配律以及负元的定义,

$$(a-b)c+bc=[(a-b)+b]c=ac$$

$$c(a-b)+cb=c[(a-b)+b]=ca$$

这样由(4),

$$(a-b)c=ac-bc \tag{7}$$

$$c(a-b)=ca-cb$$

由(7), $(a-a)a=a(a-a)=aa-aa=0$, 因此,

$$0a=a0=0 \tag{8}$$

注意,这里的 0 都是 R 的零元.

由分配律,负元的定义以及(8),

$$ab+(-a)b=(a-a)b=0,\quad ab+a(-b)=a(b-b)=0$$

因此,

$$(-a)b=a(-b)=-ab \tag{9}$$

由(9)很容易推出,

$$(-a)(-b)=ab \tag{10}$$

因为两个分配律都成立,而加法又适合结合律,所以

$$a(b_1+b_2+\cdots+b_n)=ab_1+ab_2+\cdots+ab_n \tag{11}$$

$$(b_1+b_2+\cdots+b_n)a=b_1a+b_2a+\cdots+b_na$$

由(11)可得

$$(a_1+\cdots+a_m)(b_1+\cdots+b_n)= \tag{12}$$

$$=a_1b_1+\cdots+a_1b_n+\cdots+a_mb_1+\cdots+a_mb_n$$

以上等式的右端我们有时也写作$\sum_{i=1}^{m}\sum_{j=1}^{n}a_ib_j$, 这样,

$$\left(\sum_{i=1}^{m}a_i\right)\left(\sum_{j=1}^{n}b_j\right)=\sum_{i=1}^{m}\sum_{j=1}^{n}a_ib_j$$

由(11), (8), (9), 对于任何整数 n, R 的任何 a, b 来说,

(13) $$(na)b=a(nb)=n(ab)$$

因为乘法适合结合律，n 个元的乘积有意义．跟群论里一样，n 个 a 的乘积我们用符号 a^n 来表示，并且把它叫做 a 的 n 次乘方(简称 n 次方)：

$$a^n=\overbrace{aa\cdots a}^{n\text{个}} \qquad (n\text{是正整数})$$

这样规定以后，对于任何正整数 m,n，与 R 的任何元 a 来说，

(14) $$a^m a^n=a^{m+n}$$
$$(a^m)^n=a^{mn}$$

由以上各条我们可以看出，中学代数的计算法在一个环里差不多都可适用．只有很少的几种普通计算法在一个环里不一定对，这一点我们在下一节里讨论．

习　　题

1．证明，本节内所给的加群的一个子集作成一个子群的条件是充分而且必要的．

2．$R=\{0,a,b,c\}$，加法和乘法由以下两个表给定：

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

×	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

证明，R 作成一个环．

§2．交换律、单位元、零因子、整环

若干普通计算法在一个一般的环里不成立，他们要在有附加条件的环里才能成立．我们在这一节里先讨论环的三种重要附加条件．

交换律 在环定义里我们没有要求环的乘法适合交换律，所以在一个环里 ab 未必等于 ba. 比方说，上一节的习题 2 里的环就是这样的一个. 这种环的例子我们以后还要碰到.

但一个环的乘法可能是适合交换律的，比方说整数环.

定义 一个环 R 叫做一个交换环，假如

$$ab=ba$$

不管 a,b 是 R 的哪两个元.

在一个交换环里，对于任何正整数 n 以及环的任意两个元 a,b 来说，都有

$$a^n b^n=(ab)^n$$

单位元 在群论里我们已经看到了单位元的重要性. 在环的定义里我们没有要求一个环要有一个对于乘法来说的单位元. 但一个环假如有这样一个元，我们可以想象，这个元也会占一个很重要的地位.

定义 一个环 R 的一个元 e 叫做一个单位元，假如对于 R 的任意元 a 来说，都有

$$ea=ae=a$$

一般，一个环未必有一个单位元.

例 1 $R=\{$所有偶数$\}$. R 对于普通加法和乘法来说显然作成一个环. 但 R 没有单位元.

但在特殊的环里单位元是会存在的，比方说整数环的 1.

一个环 R 如果有单位元，它只能有一个. 因为，假如 R 有两个单位元 e 和 e'，那么

$$ee'=e=e'$$

在一个有单位元的环里，这个唯一的单位元习惯上常用 1 来表示，我们以下也采取这种表示方法. 当然，一个环的 1 一般不是普通整数 1.

我们暂时只看有单位元的环.

在这种环里我们同群论里一样，如下地规定一个元 a 的零次方：

$$a^0=1$$

我们也规定什么叫做一个元的(对乘法来说的)逆元.

定义 一个有单位元环的一个元 b 叫做元 a 的一个**逆元**，假如

$$ba=ab=1$$

一个元 a 最多只能有一个逆元. 因为，假如 a 有两个逆元 b 和 b'，那么

$$\begin{aligned} bab' &= b(ab')=b1=b \\ &=(ba)b'=1b'=b' \end{aligned}$$

当然一个元 a 未必有逆元. 象整数环是一个有单位元的环，但除了 ±1 以外，其他的整数都没有逆元.

如果一个元 a 有逆元，那么这个唯一的逆元我们同群论里一样用 a^{-1} 来表示，并且规定

$$a^{-n}=(a^{-1})^n$$

这样规定以后，对这个 a 来说，公式

$$a^m a^n=a^{m+n},\quad (a^m)^n=a^{mn}$$

就对于任何整数 m,n 都成立了.

零因子 我们证明过，一个环的两个元 a,b 之间如果有一个是零，那么 ab 也等于零. 可是

$$(1)\qquad ab=0 \Longrightarrow a=0 \text{ 或 } b=0$$

这一条普通的计算规则在一个一般环里并不一定成立.

例 2 $R=\{$所有模 n 的剩余类$\}$. 我们替 R 规定过一种加法

$$[a]+[b]=[a+b]$$

并且知道 R 对于这个加法来说作成一个加群. 现在我们要替 R 规

定一个乘法. 我们规定:

(2) $$[a][b]=[ab]$$

模 n 的剩余类是由整数间的等价关系

$$a\equiv b(n),\ \text{当而且只当}\ n\mid a-b\ \text{的时候}$$

所决定的. 若是

$$[a]=[a'],\ [b]=[b']$$

那么由等式

$$ab-a'b'=a(b-b')+(a-a')b'$$

容易证明

$$[ab]=[a'b']$$

所以(2)是一个 R 的乘法. 由上述加法和乘法的定义易见: 乘法适合结合律, 并且两个分配律都成立. 因此 R 作成一个环. 这个环叫做模 n 的**剩余类环**.

若是 n 不是素数:

$$n=ab,\ n\nmid a,\ n\nmid b$$

那么在环 R 里

$$[a]\neq[0],[b]\neq[0],\text{但}[a][b]=[ab]=[n]=[0]$$

因为[0]正是 R 的零元, 这就是说, (1)在 R 里不成立.

定义 若是在一个环里

$$a\neq 0, b\neq 0\ \text{但}\ ab=0$$

我们就说, a 是这个环的一个**左零因子**, b 是一个**右零因子**.

我们要注意, 一个环若是交换环, 它的一个左零因子当然也是一个右零因子. 但在非交换环中, 一个零因子未必同时是左也是右零因子. 比方上节习题 2 里的 a 同时是左也是右零因子, 可是 b 和 c 就仅是右零因子而不是左零因子.

一个环当然可以没有零因子, 比方说整数环. 显然, **在而且只在一个没有零因子的环里(1)式才会成立.**

例 3 由高等代数知，一个数域 F 上一切 $n\times n$ 矩阵对于矩阵的加法和乘法来说，做成一个有单位元的环．当 $n\geqslant 2$ 时，这个环是非交换环，并有零因子．

零因子存在不存在同消去律成立不成立也有密切关系．

定理 在一个没有零因子的环里两个消去律都成立：

$$a\neq 0,\ ab=ac\Longrightarrow b=c$$

$$a\neq 0,\ ba=ca\Longrightarrow b=c$$

反过来，在一个环里如果有一个消去律成立，那么这个环没有零因子．

证明 假定环 R 没有零因子．因为

$$ab=ac\Longrightarrow a(b-c)=0$$

在上述假定之下，

$$a\neq 0,\ ab=ac\Longrightarrow b-c=0\Longrightarrow b=c$$

同样可证，

$$a\neq 0,\ ba=ca\Longrightarrow b=c$$

这样，在 R 里两个消去律都成立．

反过来，假定在环 R 里第一个消去律成立．因为

$$ab=0\Longrightarrow ab=a0$$

在上述假定之下，

$$a\neq 0,\ ab=0\Longrightarrow b=0$$

这就是说，R 没有零因子．第二个消去律成立的时候，情形一样．证完．

推论 在一个环里如果有一个消去律成立，那么另一个消去律也成立．

以上我们认识了一个环可能适合的三种附加条件：第一个是乘法适合交换律，第二个是单位元的存在，第三个是零因子的不存在．一个环当然可以同时适合一种以上的附加条件，同时适合

以上三种附加条件的环特别重要.

定义 一个环 R 叫做一个**整环**，假如

1．乘法适合交换律：

$$ab=ba$$

2．R 有单位元 1：

$$1a=a1=a$$

3．R 没有零因子：

$$ab=0\Longrightarrow a=0 \text{ 或 } b=0$$

这里 a,b 可以是 R 的任意元.

整数环显然是一个整环.

习　题

1．证明，二项式定理

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\cdots+b^n$$

在交换环中成立.

2．假定一个环 R 对于加法来说作成一个循环群. 证明，R 是交换环.

3．证明，对于有单位元的环来说，加法适合交换律是环定义里其它条件的结果（利用 $(a+b)(1+1)$）.

4．找一个我们还没有提到过的有零因子的环.

5．证明，由所有实数 $a+b\sqrt{2}$（a, b 是整数）作成的集合对于普通加法和乘法来说是一个整环.

§3．除环、域

现在我们要谈到一个环可能适合的另一个附加条件. 我们已经在环里下过了逆元的定义，并且知道环的一个任意元不一定有一个逆元. 我们问，在一个环里会不会每一个元都有一个逆元？在极特殊的情形下这是可能的.

例 1　R 只包括一个元 a，加法和乘法是：

$$a+a=a,\quad aa=a$$

R 显然是一个环．这个环 R 的唯一的元 a 有一个逆元，就是 a 本身．

但当环 R 至少有两个元的时候情形就不同了．这样，R 至少有一个不等于零的元 a，因此 $0a=0\neq a$．这就是说，0 不会是 R 的单位元．但 $0b=0$，不管 b 是 R 的哪一个元．由此知道，R 的 0 不会有逆元．

例 1 的环没有多大意思，我们可以不去管它．现在专看至少有两个元的环．这种环的零元不会有逆元我们已经知道．我们进一步问，除了零元以外，其它的元会不会都有一个逆元？这是可能的．

例 2　全体有理数作成的集合对于普通加法和乘法来说显然是一个环．这个环的一个任意元 $a\neq 0$ 显然有逆元 $\frac{1}{a}$．

定义　一个环 R 叫做一个除环，假如

1．R 至少包含一个不等于零的元；

2．R 有一个单位元；

3．R 的每一个不等于零的元有一个逆元．

定义　一个交换除环叫做一个域．

照我们的定义，例 2 的全体有理数的集合是一个域．同样，全体实数或全体复数的集合对于普通加法和乘法来说也各是一个域．这都是交换除环的例子．非交换除环的例子在下面就要看到．我们先看一看，除环以及域的几个最重要的性质．

(a) 一个除环没有零因子．因为：

$$a\neq 0,\ ab=0\Longrightarrow a^{-1}ab=b=0$$

(b) 一个除环 R 的不等于零的元对于乘法来说作成一个群

R^*. 因为：由于(a)，R^* 对于乘法来说是闭的；由于环的定义，乘法适合结合律；R^* 有单位元，就是 R 的单位元；由于除环的定义，R^* 的每一个元有一个逆元. R^* 叫做**除环 R 的乘群**. 这样，一个除环是由两个群，加群与乘群，凑合而成的；分配律好象是一座桥，使得这两个群中间发生一种联系.

由于(a)，(b)，在一个除环 R 里，方程

$$ax=b \text{ 和 } ya=b \quad (a, b\in R, a\neq 0)$$

各有一个唯一的解，就是 $a^{-1}b$ 和 ba^{-1}. 在普通数的计算里，我们把以上两个方程的相等的解用 $\frac{b}{a}$ 来表示，并且说，$\frac{b}{a}$ 是用 a 除 b 所得的结果. 因此，在除环的计算里，我们说，$a^{-1}b$ 是用 a 从左边去除 b，ba^{-1} 是用 a 从右边去除 b 的结果. 这样，在一个除环里，只要元 $a\neq 0$，我们就可以用 a 从左或从右去除一个任意元 b. 这就是除环这个名字的来源. 我们有区分从左除和从右除的必要，因为在一个除环里，$a^{-1}b$ 未必等于 ba^{-1}.

现在我们看一个域. 在一个域里，$a^{-1}b=ba^{-1}$. 因此我们不妨把这两个相等的元又用 $\frac{b}{a}$ 来表示. 这时我们就可以得到普通计算法：

(i) $\frac{a}{b}=\frac{c}{d}$，当而且只当 $ad=bc$ 的时候

(ii) $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$

(iii) $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$

我们只证明(i)：

$$\frac{a}{b}=\frac{c}{d}\Longrightarrow bd\frac{a}{b}=bd\frac{c}{d}\Longrightarrow ad=bc$$

并且因为消去律在一个域内成立(域无零因子),

$$\frac{a}{b}\neq\frac{c}{d}\Longrightarrow bd\frac{a}{b}\neq bd\frac{c}{d}\Longrightarrow ad\neq bc$$

其余两个式子的成立也只要两边用 bd 一乘就可以看出.

我们现在给一个非交换除环的例.

例 3 $R=\{$所有复数对$(\alpha,\beta)\}$. 这里

$(\alpha_1,\beta_1)=(\alpha_2,\beta_2)$, 当而且只当 $\alpha_1=\alpha_2,\beta_1=\beta_2$ 的时候.

R 的加法和乘法是

$$(\alpha_1,\beta_1)+(\alpha_2,\beta_2)=(\alpha_1+\alpha_2,\beta_1+\beta_2)$$

$$(\alpha_1,\beta_1)(\alpha_2,\beta_2)=(\alpha_1\alpha_2-\beta_1\bar{\beta}_2,\alpha_1\beta_2+\beta_1\bar{\alpha}_2)$$

这里 $\bar{\alpha}$ 表示的是 α 的共轭数:

$$\alpha=a_1+a_2i,\bar{\alpha}=a_1-a_2i\quad(a_1,a_2\text{ 是实数})$$

对于加法来说, R 显然作成一个加群. 用简单的计算, 我们可以验证, 乘法适合结合律, 并且两个分配律都成立. 因此 R 作成一个环.

R 有一个单位元, 就是 $(1,0)$. 我们看 R 的一个元

$$(\alpha,\beta)=(a_1+a_2i,b_1+b_2i),\quad(a_1,a_2,b_1,b_2\text{ 是实数})$$

由于 $\quad(\alpha,\beta)(\bar{\alpha},-\beta)=(\bar{\alpha},-\beta)(\alpha,\beta)=(\alpha\bar{\alpha}+\beta\bar{\beta},0)$

而 $\quad\alpha\bar{\alpha}+\beta\bar{\beta}=a_1^2+a_2^2+b_1^2+b_2^2\neq0,\qquad$ 除非 $\alpha=\beta=0$

所以只要 (α,β) 不是 R 的零元 $(0,0)$, 它就有一个逆元

$$\left(\frac{\bar{\alpha}}{\alpha\bar{\alpha}+\beta\bar{\beta}},\frac{-\beta}{\alpha\bar{\alpha}+\beta\bar{\beta}}\right)$$

这样, R 是一个除环.

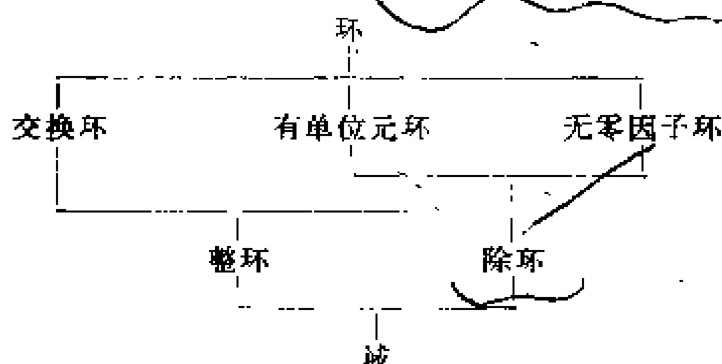
R 不是交换环. 我们算一个例子:

$$(i,0)(0,1)=(0,i),(0,1)(i,0)=(0,-i)$$

$$(i,0)(0,1)\neq(0,1)(i,0)$$

这个环叫做**四元数除环**.

到现在为止，我们已经把几种最常见的适合附加条件的环都稍微谈到了一下．为了能够把它们的隶属关系看得更清楚一点起见，我们列一个表．我们要注意，一个域一定是一个整环．



以下我们用到最多的是整环和域．

习　　题

1．$F=\{$所有复数 $a+bi$，(a，b 是有理数)$\}$．证明，F 对于普通加法和乘法来说是一个域．

2．$F=\{$所有实数 $a+b\sqrt{3}$，(a，b 是有理数)$\}$．证明，F 对于普通加法和乘法来说是一个域．

3．证明，一个至少有两个元而且没有零因子的有限环是一个除环．

4．证明，例 3 的乘法适合结合律．

5．验证，四元数除环的任意元 $(a+bi, c+di)$，这里 a, b, c, d 是实数，可以写成

$$(a,0)+(b,0)(i,0)+(c,0)(0,1)+(d,0)(0,i)$$

的形式．

§4．无零因子环的特征

我们以上看到了在各种环里有哪些普通计算规则是可以适用的．有一种普通计算规则不但在一般环里，就是在适合条件比较最强的环——域里面也还不一定能够适用，就是规则

(1) $$a\neq 0\Longrightarrow ma=\overbrace{a+a+\cdots+a}^{m\text{个}}\neq 0$$

例 1 我们看一个模 p(p 是素数)的剩余类环 F. 我们说，F 是一个域.

我们只须证明F的不等于零的元作成一个乘群 F^*. 因为乘法适合结合律，而 F^* 又是一个有限集合，F^*作成乘群的条件是：I F^*对于乘法来说是闭的，Ⅲ′. 消去律成立. 但

I. 由于 p 是素数，

$$p\nmid a, p\nmid b\Longrightarrow p\nmid ab$$

这就是说， $[a]\neq[0],[b]\neq[0]\Longrightarrow[a][b]=[ab]\neq[0]$

换一句话说， $[a],[b]\in F^*\Longrightarrow[a][b]\in F^*$

Ⅲ′. $p\mid ax-ax'=a(x-x'), p\nmid a\Longrightarrow p\mid x-x'$

这就是说， $[ax]=[ax'],[a]\neq[0]\Longrightarrow[x]=[x']$

换一句话说， $[a][x]=[a][x'],[a]\in F^*\Longrightarrow[x]=[x']$

这样，F^*果然是一个乘群，而F是一个域.

在这个域里我们有

$$[a]\neq[0],\ 但\ p[a]=0$$

这一事实. 因为不管$[a]$是F的哪一个元，

$$p[a]=\overbrace{[a]+\cdots+[a]}^{p\text{个}}=[\overbrace{a+\cdots+a}^{p\text{个}}]=[pa]=0$$

现在让我们看一看，(1)所以不一定能够成立的原因何在. 假定R是一个环. 我们知道，R 的元对于加法来说作成一个加群. 在这个加群里每一个元有一个阶. 由于阶的定义，R 的一个元 a 在加群里的阶若是无限大，那么不管m是哪一个整数，$ma\neq 0$；若 a 的阶是一个有限整数 n，那么 $na=0$. 这就是说，对于R的一个不等于零的元 a 来说，(1)能不能成立，完全由 a 在加群里的阶是无限还是有限来决定：a 的阶无限，(1)成立；a 的阶有限，(1) 不

成立.

在一个环里，可能某一个不等于零的元对于加法来说的阶是无限，另一个不等于零的元的阶却是有限的.

例 2 假定 $G_1=(b)$，$G_2=(c)$是两个循环群，b 的阶无限，c 的阶是 n. G_1 同 G_2 都是交换群，它们的代数运算可以用$+$来表示. 用加群的符号，我们有

$G_1=\{$所有 hb(h 是整数)$\}$，

$$hb=0，\text{当而且只当 } h=0 \text{ 的时候}$$

$G_2=\{$所有 kc(k 是整数)$\}$，

$$kc=0，\text{当而且只当 } n|k \text{ 的时候}$$

我们作集合 $R=\{$所有符号$(hb,kc)\}$，$(hb\in G_1, kc\in G_2)$. 并替 R 规定一个加法：

$$(h_1b,k_1c)+(h_2b,k_2c)=(h_1b+h_2b,k_1c+k_2c)$$

等式右边括号里的第一个加号表示G_1的加法，第二个表示的是G_2的加法. R 对于这个加法来说，显然作成一个加群. 我们再替R规定一个乘法：

$$(h_1b,k_1c)(h_2b,k_2c)=(0,0)$$

那么R显然作成一个环.

这个环的元$(b, 0)$对于加法来说的阶是无限大，但元$(0, c)$的阶是 n.

这样，在一个一般的环里，(1)这个计算规则可能对于某一个元来说成立，对于另一个元来说又不成立.

在一个没有零因子的环里情形就不同了.

定理 1 在一个没有零因子的环R里所有不等于零的元对于加法来说的阶都是一样的.

证明 如果R的每一个不等于零的元的阶都是无限大，那么定理是对的. 假定R的某一个元 $a\neq 0$ 的阶是有限整数 n，而 b 是

R 的另一个不等于零的元. 那么，由 Ⅲ, 1, (13),

$$(na)b = a(nb) = 0$$

因此，由于 $a \neq 0$, R 无零因子，可得 $nb = 0$. 这就是说，

$$b \text{ 的阶} \leqslant a \text{ 的阶}$$

同样可得，　　　a 的阶 $\leqslant b$ 的阶

这样，　　　a 的阶 $= b$ 的阶　　　证完

定义　一个无零因子环 R 的非零元的相同的（对加法来说的）阶叫做环 R 的**特征**.

这样，一个没有零因子的环 R 的特征如果是无限大，那么在 R 里计算规则(1)永远是对的；R 的特征如果是有限整数，这个计算规则就永远不对. 特征是一个很重要的概念，因为它对环和域的构造都有决定性的作用. 现在我们进一步证明

定理 2　如果无零因子环 R 的特征是有限整数 n, 那么 n 是一个素数.

证明　假如 n 不是素数：$n = n_1 n_2$, $n \nmid n_1$, $n \nmid n_2$. 那么对于 R 的一个不等于零的元 a 来说，

$$n_1 a \neq 0, n_2 a \neq 0, \text{但} (n_1 a)(n_2 a) = (n_1 n_2) a^2 = 0$$

这与 R 没有零因子的假定冲突. 证完.

推论　整环，除环以及域的特征或是无限大，或是一个素数 p.

在一个特征是 p 的交换环里，有一条很有趣的计算法，就是

$$(a+b)^p = a^p + b^p$$

这是因为

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$$

而 $\binom{p}{i}$ 是 p 的一个倍数的原故.

习　题

1. 假定F是一个有四个元的域. 证明:

(a) F的特征是2;

(b) F的$\neq 0$或1的两个元都适合方程$x^2=x+1$.

2.* 假定$[a]$是模n的一个剩余类. 证明, 若a同n互素, 那么所有$[a]$的数都同n互素(这时我们说$[a]$同n互素).

3.* 证明, 所有同n互素的模n的剩余类对于剩余类的乘法来说作成一个群(同n互素的剩余类的个数普通用符号$\phi(n)$来表示, 并且把它叫做尤拉ϕ函数).

4.* 证明, 若是$(a,n)=1$, 那么$a^{\phi(n)}\equiv 1(n)$[费马定理].

§5. 子环、环的同态

以上我们给了几种环的定义, 并且讨论了一下在环里的计算法. 现在要谈一谈环的子集以及同态映射. 研究环当然也离不开这两个基本概念.

定义　一个环R的一个子集S叫做R的一个**子环**, 假如S本身对于R的代数运算来说作成一个环.

一个除环R的一个子集S叫做R的一个**子除环**, 假如S本身对于R的代数运算来说作成一个除环.

同样, 我们可以规定**子整环**、**子域**的概念.

一个环的一个子集S作成一个子环的条件显然是:

$$a,b\in S \Longrightarrow a-b\in S,\ ab\in S$$

一个除环的一个子集S作成一个子除环的条件显然是:

(i)　S包含一个不等于零的元;

(ii)　$$a,b\in S \Longrightarrow a-b\in S$$

$$a,b\in S,\ b\neq 0 \Longrightarrow ab^{-1}\in S$$

例1 R本身是环R的子环. 由0一个元所作成的集合也是R的子环.

例2 一个环R的可以同每一个元交换的元作成一个子环(这件事实的证明我们留给读者当作一个习题). 这个子环叫做R的中心.

关于子环我们暂时只说这一点.

现在我们看一个环R同另外一个不空集合$\bar{R}$, $\bar{R}$有两个代数运算, 一个叫做加法, 一个叫做乘法. 由Ⅰ, 8, 定理1, 2, 及Ⅱ, 4, 定理1, 我们立刻可以得到

定理1 若是存在一个R到$\bar{R}$的满射, 使得R与$\bar{R}$对于一对加法以及一对乘法来说都同态, 那么$\bar{R}$也是一个环.

以下我们若是说两个环R与$\bar{R}$同态(同构), 我们的意思永远是存在一个R到$\bar{R}$的满射(一一映射), 使得R与$\bar{R}$对于两个环的一对加法以及一对乘法来说都同态(同构).

同群的情形类似, 我们有

定理2 假定R和$\bar{R}$是两个环, 并且R与$\bar{R}$同态. 那么, R的零元的象是$\bar{R}$的零元, R的元a的负元的象是a的象的负元. 并且, 假如R是交换环, 那么$\bar{R}$也是交换环; 假如R有单位元1, 那么$\bar{R}$也有单位元$\bar{1}$, 而且$\bar{1}$是1的象.

我们要注意, 一个环有没有零因子这一个性质经过了一个同态满射是不一定可以保持的. 我们看两个例.

例3 设R是整数环, $\bar{R}$是模n的剩余类环, 那么

$$\phi: \quad a \longrightarrow [a]$$

显然是R到$\bar{R}$的一个同态满射. 我们知道, R是没有零因子的, 但当n不是素数时, $\bar{R}$有零因子.

这个例告诉我们, R没有零因子时, 与R同态的$\bar{R}$可以有.

例4 $R=\{$所有整数对$(a,b)\}$. 对于代数运算

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

来说，R显然作成一个环，现在我们用$\bar{R}$来表示整数环，那么

$$\phi: \qquad (a, b) \longrightarrow a$$

显然是一个R到$\bar{R}$的同态满射．R的零元是$(0, 0)$，而

$$(a, 0)(0, b) = (0, 0)$$

所以R有零因子．但$\bar{R}$没有零因子．

这个例告诉我们，R有零因子时，与R同态的$\bar{R}$可以没有．

但R与$\bar{R}$间若是有一个同构映射存在，这两个环的代数性质当然没有什么区别．所以有

定理 3　假定R同$\bar{R}$是两个环，并且$R \cong \bar{R}$．那么，若R是整环，$\bar{R}$也是整环；R是除环，$\bar{R}$也是除环；R是域，$\bar{R}$也是域．

在以下的讨论里，我们有时需要作一个环，使得它包含一个给定的环．碰到这种情形的时候，我们常要用到底下的关于同构环的定理 4．我们先证明

引理　假定在集合A与$\bar{A}$之间存在一个一一映射ϕ，并且A有加法和乘法．那么我们可以替$\bar{A}$规定加法和乘法，使得A与$\bar{A}$对于一对加法以及一对乘法来说都同构．

证明　假定在给定的一一映射之下，A的元x同$\bar{A}$的元$\bar{x}$对应．我们规定：

$$\bar{a} + \bar{b} = \bar{c}, \quad \text{若} \quad a + b = c$$
$$\bar{a}\bar{b} = \bar{d}, \quad \text{若} \quad ab = d$$

这样规定的法则是$\bar{A}$的加法和乘法，因为给了$\bar{a}$和$\bar{b}$，我们可以找到唯一的a和b，因而找到唯一的c和d，唯一的$\bar{c}$和$\bar{d}$．

这样规定以后，ϕ显然对于一对加法和一对乘法来说都是同构映射．证完．

定理 4　假定S是环R的一个子环，S在R里的补足集合（这

就是所有不属于S的R的元作成的集合)与另一个环$\bar{S}$没有共同元，并且$S\cong\bar{S}$. 那么存在一个与R同构的环$\bar{R}$，而且$\bar{S}$是$\bar{R}$的子环.

证明 我们假定

$$S=\{a_s, b_s, \cdots\}$$
$$\bar{S}=\{\bar{a}_s, \bar{b}_s, \cdots\}$$

并且在S与$\bar{S}$间的同构映射ϕ之下，

$$x_s \longleftrightarrow \bar{x}_s$$

R的不属于S的元我们用$a, b, \cdots$来表示. 这样，

$$R=\{a_s, b_s, \cdots | a, b, \cdots\}$$

现在我们把所有的$\bar{a}_s, \bar{b}_s, \cdots$同所有的$a, b, \cdots$放在一起，作成一个集合$\bar{R}$.

$$\bar{R}=\{\bar{a}_s, \bar{b}_s, \cdots | a, b, \cdots\}$$

并且规定一个法则

ψ: $$x_s \longrightarrow \bar{x}_s, \quad x \longrightarrow x$$

ψ显然是一个R到$\bar{R}$的满射. 我们看R的任意两个不相同的元. 这两个元若是同时属于S，或是同时属于S的补足集合，那么它们在ψ之下的象显然不相同. 若是这两个元一个属于S，一个属于S的补足集合，那么它们在ψ之下的象一个属于$\bar{S}$，一个属于S的补足集合；由于$\bar{S}$与S的补足集合没有共同元，这两个象也不相同. 这样，ψ是R与$\bar{R}$间的一一映射. 因此，由引理，我们可以替$\bar{R}$规定加法和乘法使得

$$R\cong\bar{R}$$

由$\bar{R}$的作法，$\bar{R}\supset\bar{S}$. $\bar{S}$原来有加法和乘法，并且作成一个环. 但这还不是说，$\bar{S}$是$\bar{R}$的子环. 因为$\bar{S}$是$\bar{R}$的子环的意思是，$\bar{S}$对于$\bar{R}$的代数运算来说作成一个环. 我们把$\bar{R}$的加法暂时用$\mp$来表示，$\bar{S}$和S的加法仍用$+$来表示. 假定$\bar{x}_s$，$\bar{y}_s$是$\bar{S}$的两个任意元，

并且

$$x_s + y_s = z_s$$

那么由$\bar{+}$的定义，以及由于S与$\bar{S}$同构，

$$\bar{x}_s \bar{+} \bar{y}_s = \bar{z}_s, \quad \bar{x}_s + \bar{y}_s = \bar{z}_s$$

这就是说，假如只看对于$\bar{S}$的影响，$\bar{R}$的加法与$\bar{S}$原来的加法没有什么分别．同样可以看出，$\bar{R}$的乘法与$\bar{S}$原来的乘法对于$\bar{S}$的影响也是一样的．这样，$\bar{S}$的确是$\bar{R}$的子环．证完．

习　　题

1．证明，一个环的中心是一个交换子环．

2．证明，一个除环的中心是一个域．

3．证明，有理数域是所有复数$a+bi$（a, b是有理数）作成的域$R(i)$的唯一的真子域．

4．证明，$R(i)$有而且只有两个自同构映射．

5．J_3表示模3的剩余类所作成的集合．找出加群J_3的所有自同构映射，再找出域J_3的所有自同构映射．

6．令R是四元数除环．R的子集$S=\{$一切$(a, 0)\}$，这里a是实数．显然与实数域$\bar{S}$同构．令$\bar{R}$是把R中S换成$\bar{S}$后所得集合；替$\bar{R}$规定代数运算，使$R \cong \bar{R}$．分别用i, j, k表示$\bar{R}$的元$(i, 0)$，$(0, 1)$，$(0, i)$，那么$\bar{R}$的元可以写成

$$a+bi+cj+dk \quad (a, b, c, d \text{ 是实数})$$

的形式（参看Ⅲ，3，习题5）．验证，

$$i^2 = j^2 = k^2 = -1$$

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

§6．多 项 式 环

我们已经有了一般环的定义．现在要认识一种特殊的环．这种环在数学里占一个重要的地位．

假定R_0是一个有单位元的交换环，R是R_0的子环，并且包含

R_0 的单位元. 我们在 R_0 里取出一个元 α 来,那么

$$a_0\alpha^0+a_1\alpha^1+\cdots+a_n\alpha^n=a_0+a_1\alpha+\cdots+a_n\alpha^n \quad (a_i\in R)$$

有意义,是 R_0 的一个元.

定义 一个可以写成

$$a_0+a_1\alpha+\cdots+a_n\alpha^n \quad (a_i\in R,\ n \text{ 是} \geqslant 0 \text{ 的整数})$$

形式的 R_0 的元叫做 R 上的 α 的一个**多项式**. a_i 叫做多项式的系数.

现在我们把所有 R 上的 α 的多项式放在一起,作成一个集合,这个集合我们用 $R[\alpha]$ 来表示. 我们要注意,对于 $m<n$,

$$a_0+\cdots+a_m\alpha^m=a_0+\cdots+a_m\alpha^m+0\alpha^{m+1}+\cdots+0\alpha^n$$

所以当我们只看 $R[\alpha]$ 的有限个多项式的时候,可以假定这些多项式的项数都是一样的. 因此,$R[\alpha]$ 的两个元相加相乘适合以下公式:

$$(a_0+\cdots+a_n\alpha^n)+(b_0+\cdots+b_n\alpha^n)=(a_0+b_0)+\cdots+(a_n+b_n)\alpha^n$$

$$(a_0+\cdots+a_m\alpha^m)(b_0+\cdots+b_n\alpha^n)=c_0+\cdots+c_{m+n}\alpha^{m+n}$$

这里
$$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0=\sum_{i+j=k}a_ib_j$$

这两个式子告诉我们,$R[\alpha]$ 对于加法和乘法来说都是闭的. 由于我们也有

$$-(a_0+\cdots+a_n\alpha^n)=-a_0-\cdots-a_n\alpha^n\in R[\alpha]$$

所以 $R[\alpha]$ 是一个环. $R[\alpha]$ 显然是 R_0 的包括 R 和 α 的最小子环.

定义 $R[\alpha]$ 叫做 R 上的 α 的**多项式环**.

上面的 $R[\alpha]$ 的计算法显然正是初等代数里的多项式的计算法.

对于一个任意的 α 来说,当系数 $a_0, a_1, \cdots, a_n$ 不都等于零的时候,很可能 α 的多项式

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0$$

比方说，当 $\alpha\in R$ 的时候，取 $a_0=\alpha, a_1=-1$，那么多项式

$$a_0+a_1\alpha=\alpha-\alpha=0$$

定义 R_0 的一个元 x 叫做 R 上的一个**未定元**，假如在 R 里找不到不都等于零的元 $a_0, a_1, \cdots, a_n$ 来，使得

$$a_0+a_1x+\cdots+a_nx^n=0$$

在这一节里，我们主要是讨论未定元的多项式.

根据上述定义，R 上的一个未定元 x 的多项式，(简称**一元多项式**)只能用一种方法写成

$$a_0+a_1x+\cdots+a_nx^n \quad (a_i\in R)$$

的形式(不计系数是零的项). 对于这种多项式可以如通常一样，引入次数的概念.

定义 令

$$a_0+a_1x+\cdots+a_nx^n,\ \ a_n\neq 0$$

是环 R 上一个一元多项式. 那么非负整数 n 叫做这个多项式的**次数**. 多项式 0 没有次数.

对于给定的 R_0 来说，R_0 未必含有 R 上的未定元.

例 R 是整数环，R_0 是包含所有 $a+bi$(a, b 是整数)的整环. 这时对 R_0 的每一个元 $\alpha=a+bi$ 来说，都有

$$(a^2+b^2)+(-2a)\alpha+\alpha^2=0$$

但是我们有下面的重要定理.

定理 1 给了一个有单位元的交换环 R，一定有 R 上的未定元 x 存在，因此也就有 R 上的多项式环 $R[x]$ 存在.

证明 我们分三步来证明这个定理.

1. 首先我们利用 R 来作一个环 $\bar{P}$. 我们让 $\bar{P}$ 刚好包含所有无穷序列

$$(a_0, a_1, a_2, \cdots),\ \text{这里}\ a_i\in R,\ \text{但只有有限个}\ a_i\neq 0$$

我们限定:

只在 $a_i=b_i$,$(i=0,1,2,\cdots)$时,

$$(a_0,a_1,a_2,\cdots)=(b_0,b_1,b_2,\cdots)$$

我们规定一个加法:

$$(a_0,a_1,\cdots)+(b_0,b_1,\cdots)=(a_0+b_0,a_1+b_1,\cdots)$$

显然这是一个 $\bar{P}$ 的代数运算,而且 $\bar{P}$ 对于这个加法来说作成一个加群. 这个加群的零元是$(0,0,0,\cdots)$.

我们再规定一种乘法:

$$(a_0,a_1,a_2,\cdots)(b_0,b_1,b_2\cdots)=(c_0,c_1,c_2,\cdots)$$

这里
$$c_k=\sum_{i+j=k}a_ib_j \qquad (k=0,1,2,\cdots)$$

显然这也是一个 $\bar{P}$ 的代数运算,并且这个乘法适合交换律.

这个乘法也适合结合律:叫

$$(a_0,a_1,a_2,\cdots)(b_0,b_1,b_2,\cdots)=(d_0,d_1,d_2,\cdots)$$

$$[(a_0,a_1,\cdots)(b_0,b_1,\cdots)](c_0,c_1,\cdots)=(e_0,e_1,\cdots)$$

那么,照乘法的定义,

$$d_m=\sum_{i+j=m}a_ib_j$$

$$\begin{aligned}e_n&=\sum_{m+k=n}d_mc_k\\&=\sum_{m+k=n}\left(\sum_{i+j=m}a_ib_j\right)c_k\\&=\sum_{i+j+k=n}a_ib_jc_k\end{aligned}$$

把$(a_0,a_1,\cdots)[(b_0,b_1,\cdots)(c_0,c_1,\cdots)]$计算一下,可以得到同样的结果.

这两个代数运算也适合分配律:叫

$$(a_0,a_1,\cdots)[(b_0,b_1,\cdots)+(c_0,c_1,\cdots)]=(d_0,d_1,d_2,\cdots)$$

那么,由加法和乘法的定义,

$$d_k = \sum_{i+j=k} a_i(b_j + c_j)$$
$$= \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j$$

把$(a_0, a_1, \cdots)(b_0, b_1, \cdots) + (a_0, a_1, \cdots)(c_0, c_1, \cdots)$算出来，显然会得到同样的结果.

这样$\bar{P}$作成一个交换环.

在$\bar{P}$里我们有等式

(1) $$(a_0, 0, 0, \cdots)(b_0, b_1, \cdots) = (a_0 b_0, a_0 b_1, \cdots)$$

由这个式子我们可以得到

$$(1, 0, 0, \cdots)(b_0, b_1, \cdots) = (b_0, b_1, \cdots)$$

这就是说$\bar{P}$有单位元$(1, 0, 0, \cdots)$.

2. 第二步我们利用$\bar{P}$来得到一个包含R的环P. 由等式(1)，我们可以得到

(2) $$(a, 0, 0, \cdots)(b, 0, 0, \cdots) = (ab, 0, 0, \cdots)$$

由加法的定义，我们有

(3) $$(a, 0, 0, \cdots) + (b, 0, 0, \cdots) = (a + b, 0, 0, \cdots)$$

(2)和(3)告诉我们，全体$(a, 0, 0, \cdots)$形式的$\bar{P}$的元作成一个子环$\bar{R}$，并且

$$(a, 0, 0, \cdots) \longleftrightarrow a$$

是$\bar{R}$与R间的一个同构映射. 因为R同$\bar{P}$根本没有共同元，由Ⅲ，5，定理4，我们可以用R来代替$\bar{R}$，而得到一个包含R的环P；P也是有单位元的交换环，并且P的单位元就是R的1.

3. 最后我们证明P包含R上的未定元. 我们叫

$$x = (0, 1, 0, 0, \cdots)$$

我们说，

(4) $$x^k = (\overbrace{0, \cdots, 0}^{k\text{个}}, 1, 0, \cdots)$$

当$k=1$时，这个式子显然是对的. 假定对于$k-1$，式子是对的，

那么,

$$x^k=(0,1,0,\cdots)(\overbrace{0,0,\cdots,0}^{k-1\text{个}},1,0,\cdots)$$

$$=\left(\sum_{i+j=0}a_ib_j,\sum_{i+j=1}a_ib_j,\cdots\right)$$

但这里只有 a_1 和 b_{k-1} 等于 1. 其余 a_i, b_j 都等于零, 所以除了在 $\sum_{i+j=k}a_ib_j$ 这个和里有一项 $a_1b_{k-1}=1\times1=1\neq0$ 以外, 其余到处都是零, 因此

$$x^k=(\overbrace{0,0,\cdots,0}^{k\text{个}},1,0,\cdots)$$

现在假定在 P 里,

$$a_0+a_1x+\cdots+a_nx^n=0\qquad(a_i\in R)$$

那么在 $\bar{P}$ 里

$$(a_0,0,\cdots)+(a_1,0,\cdots)x+\cdots+(a_n,0,\cdots)x^n=(0,0,\cdots)$$

这样,由(4)和(1),

$$(a_0,a_1,\cdots,a_n,0,\cdots)=(0,0,\cdots)$$

因而 $$a_0=a_1=\cdots=a_n=0$$

这正是说, x 是 R 上的未定元. 证完.

以上所说的多项式的概念很容易加以推广. 我们还是看一个有单位元的交换环 R_0, 和它的一个子环 R, R 包含 R_0 的单位元. 我们从 R_0 里任意取出 n 个元 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 来,那么我们可以作 R 上的 α_1 的多项式环 $R[\alpha_1]$, 然后作 $R[\alpha_1]$ 上的 α_2 的多项式环 $R[\alpha_1][\alpha_2]$. 这样下去,可以得到 $R[\alpha_1][\alpha_2]\cdots[\alpha_n]$. 这个环包括所有可以写成

(5) $$\sum_{i_1i_2\cdots i_n}a_{i_1i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}$$

$$(a_{i_1\cdots i_n}\in R,\text{但只有有限个 }a_{i_1\cdots i_n}\neq0)$$

形式的元.

定义 一个有(5)的形式的元叫做 R 上的 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 的一个多项式. $a_{i_1\cdots i_n}$ 叫做多项式的系数.

环 $R[\alpha_1][\alpha_2]\cdots[\alpha_n]$ 叫做 R 上的 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 的多项式环. 这个环我们也用符号 $R[\alpha_1, \alpha_2, \cdots, \alpha_n]$ 来表示.

我们容易看出, 在 $R[\alpha_1, \alpha_2, \cdots, \alpha_n]$ 里, 两个多项式相加相乘适合以下计算法:

$$\sum_{i_1\cdots i_n} a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n} + \sum_{i_1\cdots i_n} b_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}$$

$$= \sum_{i_1\cdots i_n} (a_{i_1\cdots i_n} + b_{i_1\cdots i_n})\alpha_1^{i_1}\cdots\alpha_n^{i_n}$$

$$\left(\sum_{i_1\cdots i_n} a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}\right)\left(\sum_{j_1\cdots j_n} b_{j_1\cdots j_n}\alpha_1^{j_1}\cdots\alpha_n^{j_n}\right)$$

$$= \sum_{k_1\cdots k_n} c_{k_1\cdots k_n}\alpha_1^{k_1}\cdots\alpha_n^{k_n}$$

这里 $$c_{k_1\cdots k_n} = \sum_{i_m+j_m=k_m} a_{i_1\cdots i_n} b_{j_1\cdots j_n} \quad (m=1, 2, \cdots n)$$

同上面类似, 我们有

定义 R_1 的 n 个元 $x_1, x_2, \cdots, x_n$ 叫做 R 上的**无关未定元**, 假如任何一个 R 上的 $x_1, x_2, \cdots, x$ 的多项式都不会等于零, 除非这个多项式的所有系数都等于零.

定理 2 给了一个有单位元的交换环 R 同一个正整数 n, 一定有 R 上的无关未定元 $x_1, x_2, \cdots, x_n$ 存在, 因此也就有 R 上的多项式环 $R[x_1, x_2, \cdots, x_n]$ 存在.

证明 由定理 1, 我们可以找到一个 $R[x_1, x_2, \cdots, x_n]$, 使得 x_i 是 $R[x_1, x_2, \cdots, x_{i-1}]$ 上的未定元. 我们说, 这样得来的 $x_1, x_2, \cdots, x_n$ 是 R 上的无关未定元. 这一点用归纳法可以看出: x_1 显然是 R 上的无关未定元. 假定 $x_1, x_2, \cdots, x_{n-1}$ 是 R 上的无关未定元. 我们很容易看出, 由

(6) $$\sum_{i_1\cdots i_n} a_{i_1\cdots i_n} x_1^{i_1}\cdots x_n^{i_n}=0$$

可得 $$\sum_{i_1\cdots i_n}(a_{i_1\cdots i_n} x_1^{i_1}\cdots x_{n-1}^{i_{n-1}})x_n^{i_n}=0$$

$$\sum_{i_n}\left(\sum_{i_1\cdots i_{n-1}} a_{i_1\cdots i_n} x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\right)x_n^{i_n}=0$$

这样，因为 x_n 是 $R[x_1,\cdots,x_{n-1}]$上的未定元，(6)如果成立，一定有

$$\sum_{i_1\cdots i_{n-1}} a_{i_1\cdots i_n} x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}=0 \qquad (i_n=0,1,\cdots)$$

因此，由于 $x_1,x_2,\cdots,x_{n-1}$ 是 R 上的无关未定元，可得所有

$$a_{i_1\cdots i_n}=0$$

这就是说，$x_1,x_2,\cdots,x_n$ 是 R 上的无关未定元．证完．

上述 n 个无关未定元的多项式(简称 n 元多项式)的定义与普通 n 个无关变数的多项式的定义并不相同．但这两种多项式有很类似的性质．这两种多项式的计算法相同，我们已经看到．进一步我们有

定理 3 假定 $R[x_1,x_2,\cdots,x_n]$和 $R[\alpha_1,\alpha_2,\cdots,\alpha_n]$都是有单位元的交换环 R 上的多项式环，$x_1,x_2,\cdots,x_n$ 是 R 上的无关未定元，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 R 上的任意元．那么

$$R[x_1,x_2,\cdots,x_n]\text{与}R[\alpha_1,\alpha_2,\cdots,\alpha_n]$$

同态．

证明 我们用 $f(x_1,x_2,\cdots,x_n)$ 来表示 $R[x_1,x_2,\cdots,x_n]$的元

$$\sum_{i_1\cdots i_n} a_{i_1\cdots i_n} x_1^{i_1}\cdots x_n^{i_n}$$

用 $f(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 来表示 $R[\alpha_1,\cdots,\alpha_n]$的元

$$\sum_{i_1\cdots i_n} a_{i_1\cdots i_n} \alpha_1^{i_1}\cdots \alpha_n^{i_n}$$

那么 $$f(x_1,x_2,\cdots,x_n)\longrightarrow f(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

是 $R[x_1,x_2,\cdots,x_n]$ 到 $R[\alpha_1,\alpha_2,\cdots,\alpha_n]$ 的一个满射．因为：给了一个 $R[x_1,x_2,\cdots,x_n]$ 的元 y，由于 $x_1,x_2,\cdots,x_n$ 是无关未定元，只有一种方法可以把 y 写成多项式 $f(x_1,x_2,\cdots,x_n)$．这样，依照我们的规定，y 只有一个象，就是 $f(\alpha_1,\alpha_2,\cdots,\alpha_n)$．另一方面，显然这个映射是一个满射．

由于在 $R[x_1,x_2,\cdots,x_n]$ 或 $R[\alpha_1,\alpha_2,\cdots,\alpha_n]$ 里两个多项式的相加或相乘是适合同一规律的，以上映射是同态映射．证完．

定理 3 告诉我们，若 $R[x_1,x_2,\cdots,x_n]$ 的若干个元

$$f_1(x_1,\cdots,x_n),f_2(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)$$

之间有一个由加法和乘法计算得来的关系存在，那么用一个包含 R 的交换环 R_0（R 的单位元也是 R_0 的单位元）的任意 n 个元 $\alpha_1,\cdots,\alpha_n$ 去代替 $x_1,\cdots,x_n$，这个关系仍然成立．这正是说代入的可能，但代入的可能正是普通多项式的一个重要性质．

习　题

1．证明：假定 R 是一个整环，那么 R 上的一元多项式环 $R[x]$ 也是一个整环．

2．假定 R 是模 7 的剩余类环．在 $R[x]$ 里把乘积

$$([3]x^3+[5]x-[4])([4]x^2-x+[3])$$

计算出来．

3．证明：

(i) $R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$

(ii) 若 $x_1,x_2,\cdots,x_n$ 是 R 上的无关未定元，那么每一个 x_i 都是 R 上的未定元．

4．证明：

(i) 若是 $x_1,x_2,\cdots,x_n$ 和 $y_1,y_2,\cdots,y_n$ 是 R 上的两组无关未定元，那么

$$R[x_1,x_2,\cdots,x_n]\cong R[y_1,y_2,\cdots,y_n]$$

(ii) R 上的一元多项式环 $R[x]$ 能与它的一个真子环同构．

§ 7. 理 想

现在我们回到一般环的讨论.

我们已经知道什么叫做一个子环. 在这一节里我们要讨论到一种特别重要的子环，就是理想子环. 这种子环在环论里的地位同不变子群在群论里的地位类似.

定义 环 R 的一个非空子集 $\mathfrak{A}$ 叫做一个**理想子环**，简称**理想**，假如

(i) $$a, b \in \mathfrak{A} \Longrightarrow a - b \in \mathfrak{A}$$

(ii) $$a \in \mathfrak{A},\ r \in R \Longrightarrow ra, ar \in \mathfrak{A}$$

由于(i)，一个理想 $\mathfrak{A}$ 是一个加群，由于(ii)，$\mathfrak{A}$ 对于乘法来说是闭的，所以一个理想一定是一个子环. 但(ii)不仅要求 $\mathfrak{A}$ 的两个元的乘积必须在 $\mathfrak{A}$ 里，而且进一步要求，$\mathfrak{A}$ 的一个任意元同 R 的一个任意元的乘积都必须在 $\mathfrak{A}$ 里. 所以一个理想所适合的条件比一般子环的要强一点.

我们首先要问，一个环是不是一定有理想？回答是肯定的. 因为一个环 R 至少有以下两个理想：

1. 只包含零元的集合，这个理想叫做 R 的**零理想**；
2. R 自己，这个理想叫做 R 的**单位理想**.

有的环除了这两个理想以外，没有其它理想，比方说除环.

定理 1 一个除环 R 只有两个理想，就是零理想和单位理想.

证明 假定 $\mathfrak{A}$ 是 R 的一个理想而 $\mathfrak{A}$ 不是零理想. 那么 $\mathfrak{A} \ni a \neq 0$，由理想的定义，$a^{-1}a = 1 \in \mathfrak{A}$，因而 R 的任意元 $b = b \cdot 1 \in \mathfrak{A}$. 这就是说，$\mathfrak{A} = R$. 证完.

因此，理想这个概念对于除环或域没有多大用处.

一般来说，一个环除了以上两个理想以外是会有其它理想的.

我们举两个例.

例 1 看整数环 R. 那么一个固定整数 $n\neq 0$ 的所有倍数 rn $(r\in R)$ 作成一个理想.

例 2 看一个环 R 上的一元多项式环 $R[x]$. 那么所有多项式

$$a_1x+a_2x^2+\cdots+a_nx^n \qquad (n\geqslant 1)$$

作成 $R[x]$ 的一个理想.

以上两个理想显然既不是零理想也不是单位理想.

给了一个环 R, 我们可以用以下方法来作一些 R 的理想. 我们在 R 里任意取出一个元 a 来, 利用 a 我们作一个集合 $\mathfrak{A}$, $\mathfrak{A}$ 包含所有可以写成

$$(x_1ay_1+\cdots+x_may_m)+sa+at+na \quad (x_i, y_i, s, t\in R, n \text{ 是整数})$$

形式的元. 我们说, $\mathfrak{A}$ 是 R 的一个理想. 因为: 两个这种形式的元相减显然还是一个这种形式的元; 用 R 的一个元 r 从左边去乘 $\mathfrak{A}$ 的一个元也得到一个这种形式的元, 就是

$$[(rx_1)ay_1+\cdots+(rx_m)ay_m+rat]+(rs+nr)a$$

用 r 从右边去乘 $\mathfrak{A}$ 的元, 情形一样.

$\mathfrak{A}$ 显然是包含 a 的最小的理想.

定义 上面这样的 $\mathfrak{A}$ 叫做由元 a 生成的**主理想**. 这个理想我们用符号 (a) 来表示.

以下用到最多的理想就是主理想.

一个主理想 (a) 的元的形式并不是永远像上面那样复杂.

当 R 是交换环时, (a) 的元显然都可以写成

$$ra+na \quad (r\in R, n \text{ 是整数})$$

的形式.

当 R 有单位元的时候, (a) 的元都可以写成

$$\sum x_iay_i \quad (x_i, y_i\in R)$$

的形式, 因为这时,

$$sa=sa1,\quad at=1at,\quad na=(n1)a1$$

当R既是交换环又有单位元的时候，(a)的元的形式特别简单，这时它们都可以写成

$$ra\quad (r\in R)$$

的样子．这样，例1里的理想就是由n生成的主理想(n)．

主理想的概念容易加以推广．

我们在环R里任意取出m个元$a_1, a_2, \cdots, a_m$来，利用这m个元，我们作一个集合$\mathfrak{A}$，使$\mathfrak{A}$包含所有可以写成

$$s_1+s_2+\cdots+s_m\quad (s_i\in(a_i))$$

形式的R的元．我们说$\mathfrak{A}$是R的一个理想．这一点很容易证明．我们看$\mathfrak{A}$的任意两个元a和a'，

$$a=s_1+s_2+\cdots+s_m\quad (s_i\in(a_i))$$

$$a'=s_1'+s_2'+\cdots+s'_m\quad (s'_i\in(a_i))$$

那么，由于$s_i-s_i'\in(a_i)$，

$$a-a'=(s_1-s_1')+(s_2-s_2')+\cdots+(s_m-s_m')\in\mathfrak{A}$$

并且对于R的一个任意元r来说，由于$rs_i, s_ir\in(a_i)$，

$$ra=rs_1+rs_2+\cdots+rs_m\in\mathfrak{A}$$

$$ar=s_1r+s_2r+\cdots+s_mr\in\mathfrak{A}$$

$\mathfrak{A}$显然是包含$a_1, a_2, \cdots, a_m$的最小理想．

定义 $\mathfrak{A}$叫做由$a_1, a_2, \cdots, a_m$生成的理想．这个理想我们用符号$(a_1, a_2, \cdots, a_m)$来表示．

我们举一个例．

例3 假定$R[x]$是整数环R上的一元多项式环．我们看$R[x]$的理想$(2, x)$．因为$R[x]$是有单位元的交换环，$(2, x)$由所有的元

$$2p_1(x)+xp_2(x)\qquad (p_1(x), p_2(x)\in R[x])$$

作成；换一句话说，$(2, x)$刚好包含所有多项式

(1) $$2a_0+a_1x+\cdots+a_nx^n\qquad (a_i\in R, n\geqslant 0)$$

我们证明，$(2,x)$不是一个主理想.

假定$(2,x)=(p(x))$，那么$2\in(p(x))$，$x\in(p(x))$，因而

$$2=q(x)p(x),\qquad x=h(x)p(x)$$

但

$$2=q(x)p(x)\Longrightarrow p(x)=a$$

$$x=ah(x)\qquad\Longrightarrow a=\pm 1$$

这样，$\pm 1=p(x)\in(2,x)$. 但± 1都不是(1)的形式，这是一个矛盾.

习　　题

1. 假定R是偶数环. 证明，所有整数$4r\ (r\in R)$是R的一个理想$\mathfrak{A}$. 等式$\mathfrak{A}=(4)$对不对？

2. 假定R是整数环. 证明$(3,7)=(1)$.

3. 假定例3的R是有理数域. 证明，这时$(2,x)$是一个主理想.

4. 证明，两个理想的交集还是一个理想.

5. 找出模6的剩余类环的所有理想.

6*. 一个环R的一个子集S叫做R的一个左理想，假如

(i) $\qquad a,b\in S\Longrightarrow a-b\in S$

(ii) $\qquad a\in S,\ r\in R\Longrightarrow ra\in S$

你能不能在有理数域F上的2×2矩阵环里找到一个不是理想的左理想？

§ 8. 剩余类环、同态与理想

我们已经说过，理想在环论里所占地位同不变子群在群论里所占地位类似. 在这一节里我们要说明这一点.

给了一个环R和R的一个理想$\mathfrak{A}$，若我们只就加法来看，R作成一个群，$\mathfrak{A}$作成R的一个不变子群. 这样$\mathfrak{A}$的陪集

$$[a],[b],[c],\cdots$$

作成R的一个分类. 我们现在把这些类叫做模$\mathfrak{A}$的**剩余类**. 这个分类相当于R的元间的一个等价关系，这个等价关系我们现在用符号

$$a \equiv b(\mathfrak{A})$$

来表示(念成 a 同余 b 模 $\mathfrak{A}$). 因为上述的群是加群，一个类$[a]$包含所有可以写成

$$a+u \quad (u\in\mathfrak{A})$$

的形式的元，而两个元同余的条件是：

$$a \equiv b(\mathfrak{A}), \qquad \text{当而且只当 } a-b\in\mathfrak{A} \text{ 的时候}$$

我们把所有剩余类所作成的集合叫做 $\bar{R}$, 并且规定以下的两个法则

$$[a]+[b]=[a+b]$$

$$[a][b]=[ab]$$

由于 $\mathfrak{A}$ 是一个理想，利用上述同余条件容易证明，这两个法则是 $\bar{R}$ 的代数运算.

以下两个定理与群论里的两个相当定理完全平行.

定理 1 假定 R 是一个环，$\mathfrak{A}$ 是它的一个理想，$\bar{R}$ 是所有模 $\mathfrak{A}$ 的剩余类作成的集合. 那么 $\bar{R}$ 本身也是一个环，并且 R 与 $\bar{R}$ 同态.

证明 映射

$$a \longrightarrow [a]$$

显然是 R 到 $\bar{R}$ 的一个同态映射，所以 R 与 $\bar{R}$ 同态，而 $\bar{R}$ 是一个环. 证完.

定义 $\bar{R}$ 叫做环 R 的模 $\mathfrak{A}$ 的**剩余类环**. 这个环我们用符号

$$R/\mathfrak{A}$$

来表示.

定理 2 假定 R 同 $\bar{R}$ 是两个环，并且 R 与 $\bar{R}$ 同态，那么这个同态映射的核 $\mathfrak{A}$ 是 R 的一个理想，并且

$$R/\mathfrak{A} \cong \bar{R}$$

证明 我们先证明 $\mathfrak{A}$ 是 R 的一个理想. 假定

$$a\in\mathfrak{A}, \quad b\in\mathfrak{A}$$

那么由 $\mathfrak{A}$ 的定义，在给的同态映射 ϕ 之下，

$$a \longrightarrow \bar{0},\quad b \longrightarrow \bar{0}\quad (\bar{0}\text{ 是 }\bar{R}\text{ 的零元})$$

这样，

$$a-b \longrightarrow \bar{0}-\bar{0}=\bar{0},\quad a-b\in\mathfrak{A}$$

假定 r 是 R 的任意元，而且在 ϕ 之下，$r\longrightarrow\bar{r}$．那么

$$ra \longrightarrow \bar{r}\bar{0}=\bar{0},\quad ar\longrightarrow\bar{0}\bar{r}=\bar{0}$$

$$ra\in\mathfrak{A},\quad ar\in\mathfrak{A}$$

现在我们证明 $R/\mathfrak{A}\cong\bar{R}$．我们规定一个法则

ψ:
$$[a]\longrightarrow\bar{a}=\phi(a)$$

我们说，这是一个 $R/\mathfrak{A}$ 与 $\bar{R}$ 间的同构映射．因为：

$$[a]=[b]\Longrightarrow a-b\in\mathfrak{A}\Longrightarrow\overline{a-b}=\bar{a}-\bar{b}=\bar{0}\Longrightarrow\bar{a}=\bar{b}$$

ψ 是一个 $R/\mathfrak{A}$ 到 $\bar{R}$ 的映射．但 ψ 显然是一个满射，并且

$$[a]\neq[b]\Longrightarrow a-b\notin\mathfrak{A}\Longrightarrow\overline{a-b}=\bar{a}-\bar{b}\neq\bar{0}\Longrightarrow\bar{a}\neq\bar{b}$$

ψ 是一个 $R/\mathfrak{A}$ 与 $\bar{R}$ 间的一一映射．由于

$$[a]+[b]=[a+b]\longrightarrow\overline{a+b}=\bar{a}+\bar{b}$$

$$[a][b]=[ab]\longrightarrow\overline{ab}=\bar{a}\bar{b}$$

ψ 是同构映射．证完．

以上两个定理充分地说明了理想与不变子群的平行地位．

现在让我们回过去看一看整数的剩余类环．整数的剩余类环是利用一个整数 n 同整数环 R 的元间的等价关系

$$a\equiv b\quad(n)$$

来作成的这个等价关系与利用 R 的主理想 (n) 来规定的等价关系

$$a\equiv b\quad((n))$$

一样．因为第一个等价关系是利用条件

$$n\mid a-b$$

第二个等价关系是利用条件

$$a-b\in(n)$$

来规定的，而这两个条件没有什么区别(参看Ⅱ,9)．这样，模 n 的整数的剩余类环正是 $R/(n)$．

实际上，一般的剩余类环正是整数的剩余类环的推广，所以连名称以及以上两种等价关系的符号都相同．

最后我们说明一点．我们知道，子群同不变子群经过一个同态映射是不变的(参看Ⅱ,11)．子环同理想也是这样．

定理 3 在环 R 到环 $\bar{R}$ 的一个同态映射之下，

(i) R 的一个子环 S 的象 $\bar{S}$ 是 $\bar{R}$ 的一个子环；

(ii) R 的一个理想 $\mathfrak{A}$ 的象 $\bar{\mathfrak{A}}$ 是 $\bar{R}$ 的一个理想；

(iii) $\bar{R}$ 的一个子环 $\bar{S}$ 的逆象 S 是 R 的一个子环；

(iv) $\bar{R}$ 的一个理想 $\bar{\mathfrak{A}}$ 的逆象 $\mathfrak{A}$ 是 R 的一个理想．

这个定理的证明同群论里的相当定理的证明完全类似，我们把它省去．

习 题

1*. 假定我们有一个环 R 的一个分类，而 S 是由所有的类 $[a]$，$[b]$，$[c]$，…所作成的集合．又假定

$$[x]+[y]=[x+y],\quad [x][y]=[xy]$$

规定两个 S 的代数运算．证明 $[0]$ 是 R 的一个理想，并且给定的类刚好是模 $[0]$ 的 R 的剩余类．

2. 假定 ϕ 是环 R 到环 $\bar{R}$ 的一个同态满射．证明，ϕ 是 R 与 $\bar{R}$ 间的同构映射，当而且只当 ϕ 的核是 R 的零理想的时候．

3. 假定 R 是由所有复数 $a+bi$ (a, b 是整数)作成的环．环 $R/(1+i)$ 有多少元？

§9. 最大理想

以上是关于环的一般讨论．以下我们要认识两种由一个交换环来得到一个域的重要方法．第一种就是利用最大理想的方法．

定义 一个环R的一个不等于R的理想$\mathfrak{A}$叫作一个**最大理想**，假如，除了R同$\mathfrak{A}$自己以外，没有包含$\mathfrak{A}$的理想.

例 1 我们看整数环R. 我们说，由一个素数p所生成的主理想(p)是一个最大理想. 因为：假定$\mathfrak{B}$是一个不等于(p)的R的理想，并且

$$\mathfrak{B}\supset(p)$$

那么$\mathfrak{B}$一定包含一个不能被p整除的整数q. 由于p是素数，q与p互素，所以我们可以找到整数s和t，使得

$$sp+tq=1$$

但p也属于$\mathfrak{B}$，而且$\mathfrak{B}$是理想. 所以

$$1\in\mathfrak{B},\quad \mathfrak{B}=R.$$

让我们看一看，利用最大理想，怎样可以由一个环来得到一个域. 首先给了一个环R，我们可以利用R的一个最大理想来得到一个环$\bar{R}$，使得$\bar{R}$除了零理想同单位理想以外，没有其它的理想.

引理 1 假定$\mathfrak{A}$是环R的一个理想. 剩余类环$R/\mathfrak{A}$除了零理想同单位理想以外不再有理想，当而且只当$\mathfrak{A}$是最大理想的时候.

证明 我们用ϕ来表示R到$\bar{R}=R/\mathfrak{A}$的同态满射.

我们先证明定理的条件是充分的. 假定$\mathfrak{A}$是最大理想，$\bar{\mathfrak{B}}$是$\bar{R}$的理想，并且

$$\bar{\mathfrak{B}}\neq\bar{0}$$

那么，由Ⅲ，8，定理3，在ϕ之下的$\bar{\mathfrak{B}}$的逆象$\mathfrak{B}$是R的理想，$\mathfrak{B}$显然包含$\mathfrak{A}$而且不等于$\mathfrak{A}$，所以

$$\mathfrak{B}=R,\quad \bar{\mathfrak{B}}=\bar{R}$$

这样，$\bar{R}$只有零理想同单位理想.

现在我们证明定理的条件也是必要的. 假定$\mathfrak{A}$不是最大理

想：$R\supset\mathfrak{B}\supset\mathfrak{A}$，$\mathfrak{B}$ 是 R 的理想，且既不等于 R，也不等于 $\mathfrak{A}$．那么，由Ⅲ，8，定理3，在 ϕ 之下的 $\mathfrak{B}$ 的象 $\overline{\mathfrak{B}}$ 是 $\overline{R}$ 的理想．由于 $\mathfrak{B}$ 大于 $\mathfrak{A}$，

$$\overline{\mathfrak{B}}\neq\overline{0}$$

$\overline{\mathfrak{B}}$ 也不会是 $\overline{R}$．不然的话，对于 R 的任意元 r，可以找到 $\mathfrak{B}$ 的元 b，使得

$$[r]=[b],\quad r-b\in\mathfrak{A}\subset\mathfrak{B}$$

于是，由于 $\mathfrak{B}$ 是理想，可以得到 $r\in\mathfrak{B}$，$\mathfrak{B}=R$，与假定不合．这样，$\overline{R}$ 除了零理想同单位理想以外还有理想 $\overline{\mathfrak{B}}$．证完．

我们知道，一个域只有零理想同单位理想．反过来，一个只有这两个理想的环当然还不见得是一个域．但是我们有

引理2 如果一个有单位元的交换环 R 除了零理想同单位理想以外没有其它的理想，那么 R 一定是一个域．

证明 我们看 R 的任意元 $a\neq0$．a 所生成的主理想 (a) 显然不是零理想，于是由假定，$(a)=R$．因而 R 的单位元 $1\in(a)$．但 (a) 的元都可以写成 $ra\ (r\in R)$ 的形式，所以

$$1=a'a\quad(a'\in R)$$

这样，R 的每个不等于零的元都有一个逆元，R 是一个域，证完．

由以上两个引理我们立刻可以得到

定理 假定 R 是一个有单位元的交换环，$\mathfrak{A}$ 是 R 的一个理想．$R/\mathfrak{A}$ 是一个域，当而且只当 $\mathfrak{A}$ 是一个最大理想的时候．

这样，给了一个有单位元的交换环 R，我们只要找得到 R 的一个最大理想 $\mathfrak{A}$，就可以得到一个域 $R/\mathfrak{A}$．

例2 R 是整数环，(p) 是由素数 p 所生成的主理想，那么由上面例1，$R/(p)$ 是一个域．这个结果我们在Ⅲ，4，已经得到过．

习　　题

1. 假定 R 是由所有复数 $a+bi$ (a, b 是整数) 所作成的环. 证明, $R/(1+i)$ 是一个域.

2. 我们看环 R 上的一个一元多项式环 $R[x]$. 当 R 是整数环时, $R[x]$ 的理想 (x) 是不是最大理想? 当 R 是有理数域的时候, 情形如何?

3. 我们看所有偶数作成的环 R. 证明, (4) 是 R 的最大理想, 但 $R/(4)$ 不是一个域.

4.* 我们看有理数域 F 上的全部 2×2 矩阵环 F_{22}. 证明, F_{22} 只有零理想同单位理想, 但不是一个除环.

§ 10. 商　　域

现在让我们看一看, 由一个环来得到一个域的第二种方法.

我们知道普通整数的集合作成一个环, 有理数的集合作成一个域, 而整数环是有理数域的一个子环. 现在我们问, 给了一个环 R, 是不是可以找得到一个除环或域包含这个 R. 一个环 R 要能被一个除环或域包含, 有一个必要条件, 就是 R 不能有零因子, 因为除环或域没有零因子. 当 R 是非交换环时, 这一个条件还不充分, 因为有例子告诉我们, 一个无零因子的非交换环不一定能被一个除环包含 (参看: A. Malcev, On the Immersion of an Algebraic Ring into a Field, Math. Ann. P. 113. 1936). 我们在这一节要证明, 当 R 是交换环时, 以上条件也是充分的. 我们所用的方法完全是由整数和有理数的关系得来的.

定理 1　每一个没有零因子的交换环 R 都是一个域 Q 的子环.

证明　当 R 只包含零元的时候, 定理显然是对的. 我们看至少有两个元的 R. 用 $a, b, c, \cdots$ 来表示 R 的元. 我们作一个集合

$$A=\left\{\text{所有符号}\frac{a}{b}\right\}\quad (a, b\in R,\ b\neq 0)$$

在 A 的元间我们规定一个关系

$\sim$: $$\frac{a}{b}\sim\frac{a'}{b'},\quad \text{当而且只当 } ab'=a'b \text{ 的时候}$$

很明显，

(i) $$\frac{a}{b}\sim\frac{a}{b}$$

(ii) $$\frac{a}{b}\sim\frac{a'}{b'}\Longrightarrow\frac{a'}{b'}\sim\frac{a}{b}$$

我们也有

(iii) $$\frac{a}{b}\sim\frac{a'}{b'},\quad \frac{a'}{b'}\sim\frac{a''}{b''}\Longrightarrow\frac{a}{b}\sim\frac{a''}{b''}$$

因为：由

$$\frac{a}{b}\sim\frac{a'}{b'},\quad \frac{a'}{b'}\sim\frac{a''}{b''}$$

可得 $$ab'=a'b,\quad a'b''=a''b'$$

$$(ab'')b'=(ab')b''=(a'b)b''=(a'b'')b=(a''b')b=(a''b)b'$$

但 $b'\neq 0$, R 没有零因子，所以可得

$$ab''=a''b$$

$$\frac{a}{b}\sim\frac{a''}{b'}$$

这样，$\sim$是一个等价关系.

这个等价关系把集合 A 分成若干类$\left[\frac{a}{b}\right]$. 我们作一个集合

$$Q_0=\left\{\text{所有类}\left[\frac{a}{b}\right]\right\}$$

对于 Q_0 的元我们规定

$$\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]=\left[\frac{ad+bc}{bd}\right]$$

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right]=\left[\frac{ac}{bd}\right]$$

这样规定的是 Q_0 的加法和乘法. 因为:

第一，由于 R 没有零因子，

$$b\neq 0,\ d\neq 0 \Longrightarrow bd\neq 0$$

$\left[\dfrac{ad+bc}{bd}\right]$ 和 $\left[\dfrac{ac}{bd}\right]$ 都是 Q_0 的元.

第二，假定

$$\left[\frac{a}{b}\right]=\left[\frac{a'}{b'}\right], \qquad \left[\frac{c}{d}\right]=\left[\frac{c'}{d'}\right]$$

那么

$$ab'=a'b, \qquad cd'=c'd$$

$$ab'dd'=a'bdd'$$

$$cd'bb'=c'dbb'$$

$$(ad+bc)b'd'=(a'd'-b'c')bd$$

$$\left[\frac{ad+bc}{bd}\right]=\left[\frac{a'd'-b'c'}{b'd'}\right]$$

另一方面，

$$ab'cd'=a'bc'd$$

$$(ac)(b'd')=(a'c')(bd)$$

$$\left[\frac{ac}{bd}\right]=\left[\frac{a'c'}{b'd'}\right]$$

两类相加相乘的结果与类的代表无关.

Q_0 对于加法来说作成一个加群:

(1) $$\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]=\left[\frac{c}{d}\right]+\left[\frac{a}{b}\right]$$

(2) $$\left[\frac{a}{b}\right]+\left(\left[\frac{c}{d}\right]+\left[\frac{e}{f}\right]\right)=\left[\frac{a}{b}\right]+\left[\frac{cf+de}{df}\right]$$

$$=\left[\frac{adf+bcf+bde}{bdf}\right]$$

$$\left(\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]\right)+\left[\frac{e}{f}\right]=\left[\frac{ad+bc}{bd}\right]+\left[\frac{e}{f}\right]$$
$$=\left[\frac{adf+bcf+bde}{bdf}\right]$$

(3) $$\left[\frac{0}{b}\right]+\left[\frac{c}{d}\right]=\left[\frac{bc}{bd}\right]=\left[\frac{c}{d}\right]$$

(4) $$\left[\frac{a}{b}\right]+\left[\frac{-a}{b}\right]=\left[\frac{0}{b}\right]$$

Q_0的不等于零的元对于乘法来说作成一个交换群：乘法适合交换律与结合律，显然；$\left[\frac{a}{a}\right]$是单位元；$\left[\frac{a}{b}\right]$的逆元是$\left[\frac{b}{a}\right]$。我们很容易验算，分配律也成立。

这样，Q_0作成一个域。

我们把 Q_0的所有的元

$$\left[\frac{qa}{q}\right]\ (q\text{ 是一个固定的元，}a\text{ 任意})$$

放在一起，作成一个集合 R_0，那么

$$a\longrightarrow\left[\frac{qa}{q}\right]$$

是一个 R 与 R_0间的一一映射。由于

$$\left[\frac{qa}{q}\right]+\left[\frac{qb}{q}\right]=\left[\frac{q^2(a+b)}{q^2}\right]=\left[\frac{q(a+b)}{q}\right]$$
$$\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]=\left[\frac{q(ab)}{q}\right]$$

以上映射是同构映射：

$$R\cong R_0$$

这样，由 Ⅲ，5，定理 4，有一个包含 R的域 Q 存在。证完。

这样得来的域 Q 的构造似乎相当复杂，但实际上并不如此。Q 既然是包含 R 的域，R 的一个元 $b\neq 0$ 在 Q 里有逆元 b^{-1}，因而

$$ab^{-1}=b^{-1}a=\frac{a}{b}\qquad(a,b\in R,\ b\neq 0)$$

在Q里有意义．我们有

定理2　Q刚好是由所有元

$$\frac{a}{b}\quad (a, b\in R,\ b\neq 0)$$

所作成的，这里

$$\frac{a}{b}=ab^{-1}=b^{-1}a$$

证明　要证明Q的每一个元可以写成$\frac{a}{b}$的样子，只须证明Q_0的每一个元可以写成

$$\frac{\left[\frac{qa}{q}\right]}{\left[\frac{qb}{q}\right]}=\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]^{-1}$$

的样子．我们看Q_0的任意元$\left[\frac{a}{b}\right]$．由于

$$\left[\frac{qb}{q}\right]^{-1}=\left[\frac{q}{qb}\right]$$

我们的确有

$$\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]^{-1}=\left[\frac{q^2a}{q^2b}\right]=\left[\frac{a}{b}\right]=\frac{\left[\frac{qa}{q}\right]}{\left[\frac{qb}{q}\right]}$$

至于每一个$\frac{a}{b}$都属于Q，显然．证完．

Q的元既然都可以写成$\frac{a}{b}$的样子，由Ⅲ,3,Q的元有以下性质：

$$\text{(I)}\qquad \begin{cases}\dfrac{a}{b}=\dfrac{c}{d}, \text{ 当而且只当 } ad=bc \text{ 的时候}\\[2mm] \dfrac{a}{b}+\dfrac{c}{d}=\dfrac{ad+bc}{bd}\\[2mm] \dfrac{a}{b}\cdot\dfrac{c}{d}=\dfrac{ac}{bd}\end{cases}$$

这样，Q与R的关系正同有理数域与整数环的关系一样，Q的构造并不复杂.

定义 一个域Q叫做环R的一个商域，假如Q包含R，并且Q刚好是由所有元

$$\frac{a}{b} \quad (a, b \in R, \ b \neq 0)$$

所作成的.

由定理1和2，一个有两个以上的元的没有零因子的交换环至少有一个商域.

一般，一个环很可能有两个以上的商域. 我们有

定理3 假定R是一个有两个以上的元的环，F是一个包含R的域. 那么F包含R的一个商域.

证明 在F里

$$ab^{-1} = b^{-1}a = \frac{a}{b} \quad (a, b \in R, \ b \neq 0)$$

有意义. 作F的子集

$$\bar{Q} = \left\{所有\frac{a}{b}\right\} \quad (a, b \in R, \ b \neq 0)$$

$\bar{Q}$显然是R的一个商域. 证完.

但R的每一个商域都适合计算规则(I)，而计算规则(I)完全决定于R的加法和乘法；这就是说，R的商域的构造完全决定于R的构造. 所以我们有

定理4 同构的环的商域也同构. 这样，抽象地来看，一个环最多只有一个商域.

习　题

1. 证明，一个域F是它自己的商域.
2. 详细证明本节定理3.

第四章　整环里的因子分解

在这一章里我们要讨论关于环的一个特殊问题，就是因子分解问题．因为我们的讨论相当长，因此把它自作一章．

在整数环里有一个重要的定理，就是唯一分解定理．这个定理说，一个整数可以唯一地写成若干素数的乘积．在这一章里我们要看一看，在一个抽象环 R 里这个定理是否成立；但由于在一个一般的环里去研究这个问题有相当的困难，所以我们限定 R 是一个整环．

§1．素元、唯一分解

要在一个整环里讨论因子分解，我们首先需要把整数环的整除以及素数两个概念推广到一般整环里去．

整除这个概念很容易加以推广．

定义　我们说，整环 I 的一个元 a 可以被 I 的元 b **整除**，假如在 I 里找得出元 c 来，使得

$$a=bc$$

假如 a 能被 b 整除，我们说 b 是 a 的因子，并且用符号

$$b\mid a$$

来表示．b 不能整除 a，我们用符号

$$b\nmid a$$

来表示．

把素数这个概念加以推广却没有这样简单，需要先引入几个新的概念．

定义 整环 I 的一个元 ε 叫做 I 的一个**单位**，假如 ε 是一个有逆元的元.

元 b 叫做元 a 的**相伴元**，假如 b 是 a 和一个单位 ε 的乘积：

$$b=\varepsilon a$$

我们要注意单位同单位元的区别.

一个整环至少有两个单位，就是 1 和 -1，在一般情形之下，在一个整环里常有两个以上的单位存在(参看本节习题 2).

一个整环的单位显然有以下性质：

定理 1 两个单位 ε 同 ε' 的乘积 $\varepsilon\varepsilon'$ 也是一个单位. 单位 ε 的逆元 ε^{-1} 也是一个单位.

现在我们看一个整环 I 的一个任意单位 ε 和一个任意元 a. 那么

$$a=\varepsilon(\varepsilon^{-1}a)=\varepsilon^{-1}(\varepsilon a)$$

这就是说，一个任意元 a 可以被每一个单位 ε 和 a 的每一个相伴元 εa 整除. 我们把这种永远存在的因子同其它的因子区别一下.

定义 单位以及元 a 的相伴元叫做 a 的**平凡因子**. 其余的 a 的因子，假如还有的话，叫做 a 的**真因子**.

现在让我们看一看，一个普通素数 p 有些什么性质. 一个素数 p 并不是绝对不能被任何整数整除，因为 ±1 同 $\pm p$ 都可以整除 p. 但除了这四个数以外素数 p 没有其它因子. 依照上面的规定，±1 都是整数环的单位，$+p=1\cdot p$，$-p=(-1)p$ 都是 p 的相伴元，所以我们可以说，素数 p 的一个性质是，它只有平凡因子. 素数 p 还有另外一个性质，就是 $p\neq0$ 或 ±1. 依照素数的这些性质我们下

定义 整环 I 的一个元 p 叫做一个**素元**，假如 p 既不是零元，也不是单位，并且 p 只有平凡因子.

按照这个定义以下事实成立：

定理 2 单位 ε 同素元 p 的乘积 εp 也是一个素元.

证明 由于 $\varepsilon\neq0$, $p\neq0$, 而整环没有零因子; 所以 $\varepsilon p\neq0$. εp 也不会是单位, 不然的话

$$1=\varepsilon'(\varepsilon p)=(\varepsilon'\varepsilon)p$$

p 是单位, 与假定不合.

现在假定 b 是 εp 的因子, 并且 b 不是单位. 那么

$$\varepsilon p=bc, \quad p=b(\varepsilon^{-1}c)$$

$$b\mid p$$

但 p 是素元, b 不是单位, 因此 b 一定是 p 的相伴元:

$$b=\varepsilon''p=(\varepsilon''\varepsilon^{-1})(\varepsilon p) \quad (\varepsilon'' \text{是单位})$$

这就是说, b 是 εp 的相伴元, 因为由定理 1, $\varepsilon''\varepsilon^{-1}$ 是单位. 这样 εp 只有平凡因子. 证完.

定理 3 整环中一个不等于零的元 a 有真因子的充分而且必要条件是:

$$a=bc$$

b 和 c 都不是单位.

证明 若 a 有真因子 b, 那么

$$a=bc$$

这里的 b 由真因子的定义不是单位. c 也不是单位, 不然的话 $b=ac^{-1}$, b 是 a 的相伴元, 与 b 是 a 的真因子的假定不合.

反过来, 假定

$$a=bc$$

b 和 c 都不是单位. 这时 b 不会是 a 的相伴元, 不然的话

$$b=\varepsilon a, \quad a=\varepsilon ac, \quad 1=\varepsilon c$$

c 是单位, 与假定不合. 这样, b 既不是单位, 也不是 a 的相伴元, b 是 a 的真因子. 证完.

推论 假定 $a\neq0$, 并且 a 有真因子 b: $a=bc$. 那么 c 也是 a

的真因子.

证明 由定理 3 的证明的前半，c 不是单位. 由定理 3 的证明的后半，c 是 a 的一个真因子. 证完.

已经有了素元的定义，让我们现在看一看，在什么情形之下可以说，一个元 a 可以唯一地分解成素元的乘积. 首先我们必须要求，a 可以分解成有限个素元的乘积：

$$a=p_1p_2\cdots p_n \quad (p_i \text{ 是素元})$$

不然的话，我们根本无法讨论 a 是不是能唯一地分解. 可是 a 能够写成以上的乘积，也就能够写成以下的素元的乘积：

$$a=p_2p_1\cdots p_n$$

$$a=(\varepsilon p_1)(\varepsilon^{-1}p_2)\cdots p_n \quad (\varepsilon \text{ 是任意单位})$$

假如我们把以上的几种分解看作不一样的，那么只要一个元能够写成两个以上的素元的乘积，这个元就不能有唯一的分解；这样我们的问题就没有多大意义了. 因此我们下以下

定义 我们说，一个整环 I 的一个元 a 在 I 里有**唯一分解**，假如以下条件能被满足：

（i） $a=p_1p_2\cdots p_r$ （p_i 是 I 的素元）

（ii） 若同时

$$a=q_1q_2\cdots q_s \quad (q_i \text{ 是 } I \text{ 的素元})$$

那么 $r=s$

并且我们可以把 q_i 的次序掉换一下，使得

$$q_i=\varepsilon_i p_i \quad (\varepsilon_i \text{ 是 } I \text{ 的单位})$$

依照这个定义，一个整环的零元和单位一定不能唯一地分解，因为第一个条件就不能被满足. 假如我们把零写成若干个元的乘积：

$$0=a_1a_2\cdots a_n$$

那么某一个 a_i 一定是 0，但 0 不是素元. 假如我们能把一个单

位 ε 写成若干个元的乘积：

$$\varepsilon=a_1a_2\cdots a_n$$

那么 $$1=a_1(\varepsilon^{-1}a_2\cdots a_n)$$

a_1 是一个单位，但单位不是素元.

所以唯一分解问题的研究对象只能是既不等于 0 也不是单位的元(我们说整数都能唯一分解，也没有把 0 同 ±1 算上).

现在我们就问，一个整环的不等于零也不是单位的元是不是都有唯一分解呢？下例告诉我们不是的.

例 $I=\{$所有复数 $a+b\sqrt{-3}$ (a, b 是整数)$\}$.

I 显然是一个整环. I 的元都是复数，利用复数的绝对值我们很容易得到以下事实.

(1) I 的一个元 ε 是一个单位，当而且只当 $|\varepsilon|^2=1$ 的时候. I 只有两个单位，就是 ±1.

假定 $\varepsilon=a+b\sqrt{-3}$ 是一个单位，那么

$$1=\varepsilon\varepsilon',\quad |1|^2=|\varepsilon|^2|\varepsilon'|^2,\quad 1=|\varepsilon|^2|\varepsilon'|^2$$

但 $|\varepsilon|^2=a^2+3b^2$ 是一个正整数，同样 $|\varepsilon'|^2$ 也是一个正整数，因此有 $|\varepsilon|^2=1$. 反过来看，假定

$$|\varepsilon|^2=a^2+3b^2=1$$

那么 $b=0$，$a=\pm1$；这就是说，$\varepsilon=\pm1$ 而显然是单位.

(2) 适合条件 $|\alpha|^2=4$ 的 I 的元 α 一定是素元.

首先，既然 $|\alpha|^2=4$，$\alpha\neq0$；并且由(1)，α 也不是单位. 假定 β 是 α 的因子：

$$\beta=a+b\sqrt{-3},\quad \alpha=\beta\gamma$$

那么 $$4=|\beta|^2|\gamma|^2$$

但不管 a, b 是什么整数，$|\beta|^2=a^2+3b^2\neq2$，因此

$$|\beta|^2=1 \text{ 或 } 4$$

若是 $|\beta|^2=1$，由(1)，β 是单位. 若是 $|\beta|^2=4$，那么 $|\gamma|^2=1$，

γ 是单位，因而

$$\beta=\gamma^{-1}\alpha$$

β 是 α 的相伴元．这样 α 只有平凡因子，α 是素元．

现在我们看 I 的元 4．显然

(A) $$4=2\cdot 2=(1+\sqrt{-3})(1-\sqrt{-3})$$

因为 $|2|^2=4$，$|1+\sqrt{-3}|^2=4$，$|1-\sqrt{-3}|^2=4$，

由(2)，2，$1+\sqrt{-3}$，$1-\sqrt{-3}$ 都是 I 的素元．这就是说，(A)表示 4 在 I 里的两种分解．但由 (1)，$1-\sqrt{-3}$ 和 $1-\sqrt{-3}$ 都不是 2 的相伴元，因而按照定义，以上两种分解不同．这样，4 在 I 里有两种不同的分解．

习　　题

1．证明，0 不是任何元的真因子．

2．我们看以下的整环 I，I 刚好包含所有可以写成

$$\frac{m}{2^n}\quad (m \text{ 是任意整数}, n\geqslant 0 \text{ 的整数})$$

形式的有理数．I 的哪些个元是单位，哪些个元是素元？

3．I 是刚好包含所有复数

$$a+bi\quad (a, b \text{ 是整数})$$

的整环．证明 5 不是 I 的素元．5 有没有唯一分解？

§ 2．唯一分解环

由于上一节的例我们知道，在一个整环里唯一分解定理未必成立．但是我们也知道，在有些整环里，比方说整数环里，这个定理是成立的．

定义　一个整环 I 叫做一个**唯一分解环**，假如 I 的每一个既不等于零又不是单位的元都有唯一分解．

在这一节里我们先看一看，一个唯一分解环有些什么重要

性质.

定理 1 一个唯一分解环有以下性质:

(iii) 若一个素元 p 能够整除 ab,那么 p 能够整除 a 或 b.

证明 p 能整除 ab,

$$ab = pc$$

我们先假定,a 和 b 都不是零元,也都不是单位. 这时 c 显然不等于零. 我们说 c 也不是一个单位. 不然的话

$$ab = p\varepsilon \quad (\varepsilon = c \text{ 是一个单位})$$

而由 IV,1,定理 2,$p\varepsilon$ 是素元. 这就是说,素元 $p\varepsilon$ 可以写成两个非单位的乘积,因而有真因子. 这是矛盾.

c 既不是零又不是单位,由唯一分解环的定义,

$$c = p_1p_2\cdots p_n \quad (p_i \text{ 是素元})$$

另一方面

$$a = q_1q_2\cdots q_r,\quad b = q_1'q_2'\cdots q_s' \quad (q_i, q_i' \text{ 是素元})$$

这样,

$$q_1q_2\cdots q_rq_1'q_2'\cdots q_s' = pp_1p_2\cdots p_n$$

由唯一分解的定义,p 一定是某一个 q_i 或某一个 q_i' 的相伴元. 若 p 是某一个 q_i 的相伴元,那么

$$pe'' = q_i \quad (e'' \text{ 是单位})$$

$$a = q_1q_2\cdots q_{i-1}(pe'')q_{i+1}\cdots q_r,\quad p|a.$$

同样,若 p 是某一个 q_i' 的相伴元,那么 $p|b$. 这样,p 的确能够整除 a,b 中的一个.

当 a,b 之中有一个是零或是单位的时候,定理也是对的. 若 $a=0$,那么 $p|a$. 若 a 是单位,那么

$$b = p(ca^{-1}),\quad p|b$$ 证完

性质(iii)的重要性由以下定理可以看出.

定理 2 假定一个整环 I 有以下性质:

(i) I 的每一个既不是零也不是单位的元 a 都有一个分解

$$a=p_1p_2\cdots p_r \quad (p_i \text{ 是 } I \text{ 的素元})$$

(iii) I 的一个素元 p 若能整除 ab，那么 p 能整除 a 或 b. 这时 I 一定是一个唯一分解环.

证明 我们看 I 的一个不等于零也不是单位的元 a. 由性质(i)，a 有一个分解

$$a=p_1p_2\cdots p_r \quad (p_i \text{ 是素元})$$

我们须要证明，a 有唯一分解；就是说，假定我们也有

$$a=q_1q_2\cdots q_s \quad (q_i \text{ 是素元})$$

那么 $r=s$，并且我们可以把这些 q 的次序掉换一下，使得 q_i 是 p_i 的相伴元.

我们用归纳法. 先证当 $r=1$ 的时候，a 有唯一分解. 这时

$$a=p_1=q_1q_2\cdots q_s$$

若是 $s\neq 1$，那么

$$p_1=q_1(q_2\cdots q_s)$$

其中 q_1 不是单位，而 $q_2\cdots q_s$ 作为素元的乘积也不是单位. 这就是说，素元 p 可以写成两个非单位的乘积，这不可能. 所以 $s=1=r$，$p_1=q_1$.

现在假定，能写成 $\leqslant r-1$ 个素元的乘积的元都有唯一分解. 在这个假定之下，我们看一个有象上面的两种分解的元 a:

$$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s$$

由性质(iii)，p_1 能够整除某一个 q_i；把 q_i 的次序换一换，我们可以假定 $p_1|q_1$. 但 q_1 是素元，p_1 不是单位，所以

$$p_1=\varepsilon q_1, \quad q_1=\varepsilon^{-1}p_1 \quad (\varepsilon \text{ 是单位})$$

这样

$$\varepsilon q_1p_2\cdots p_r=q_1q_2\cdots q_s$$

$$b=(\varepsilon p_2)\cdots p_r=q_2q_3\cdots q_s$$

这里 b 是 $r-1$ 个素元的乘积，所以依照归纳法的假定，

$$r-1=s-1$$

而且我们可以把 q_i 的次序掉换一下，使得

$$q_2=\varepsilon_2'(\varepsilon p_2),q_3=\varepsilon_3'p_3,\cdots,q_r=\varepsilon_r'p_r \quad (\varepsilon_i' \text{ 是单位})$$

这样我们得到

$$s=r$$

$$q_1=\varepsilon^{-1}p_1,q_2=(\varepsilon\varepsilon_2')p_2,q_3=\varepsilon_3'p_3,\cdots,q_r=\varepsilon_r'p_r$$ 证完

由定理 1,2，我们也可以用条件(i)，(iii)来作唯一分解环的定义.

唯一分解环的另一重要性质就是最大公因子的存在.

定义 元 c 叫做元 $a_1,a_2,\cdots,a_n$ 的**公因子**，假如 c 同时能够整除 $a_1,a_2,\cdots,a_n$.

元 a_1, a_2, $\cdots$, a_n 的一个公因子 d 叫做 $a_1,a_2,\cdots$, a_n 的**最大公因子**，假如 d 能够被 $a_1,a_2,\cdots,a_n$ 的每一个公因子 c 整除.

定理 3 一个唯一分解环 I 的两个元 a 和 b 在 I 里一定有最大公因子. a 和 b 的两个最大公因子 d 和 d' 只能差一个单位因子：

$$d'=\varepsilon d \quad (\varepsilon \text{ 是单位})$$

证明 若 a,b 之中有一个是零，比方说 $a=0$，那么 b 显然是一个最大公因子. 若是 a,b 之中有一个是单位，比方说 a 是单位，那么 a 显然是最大公因子.

现在看 a 和 b 都不是零也都不是单位时的情形. 这时

$$a=q_1q_2\cdots q_r, \quad b=q_1'q_2'\cdots q_s' \quad (q_i,q_i' \text{ 是素元})$$

q_i 同 q_i' 这 $r+s$ 个元中间的某一个可能是其它一个的相伴元. 假定在这 $r+s$ 个元中间有 n 个元互相不是相伴元，而其它的元都是这 n 个元中的某一个的相伴元. 把这 n 个元叫做 $p_1,p_2,\cdots,p_n$，那么

$$a=\varepsilon_a p_1^{h_1}p_2^{h_2}\cdots p_n^{h_n} \quad (\varepsilon_a \text{ 是单位}, h_i\geqslant 0)$$

$$b=\varepsilon_b p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n} \quad (\varepsilon_b \text{ 是单位}, k_i\geqslant 0)$$

用 l_i 来表示 h_i 与 k_i 中较小的一个（$h_i=k_i$ 的时候就叫 $l_i=h_i$），

而作元

$$d = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$$

那么显然 $d|a, d|b$. 假定 c 也是 a 同 b 的公因子. 若是 c 是单位, c 当然能够整除 d. 若是 c 不是单位, 那么

$$c = p_1' p_2' \cdots p_t' \quad (p_i' \text{ 是素元})$$

由于 $c|a$, 每一个 $p_i'|a$, 于是由性质(iii), p_i' 能整除某一 p_j, 而是 p_j 的相伴元, 所以

$$c = \varepsilon_c p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \quad (\varepsilon_c \text{ 是单位}, m_i \geqslant 0)$$

但 $c|a$, 并且 p_i, p_j 互相不是相伴元, 因此 $m_i \leqslant h_i$. 同理, 由 $c|b$, 可得 $m_i \leqslant k_i$. 这就是说, $m_i \leqslant l_i$, $c|d$. 这样, 我们证明了最大公因子 d 的存在.

假定 d' 也是 a 和 b 的最大公因子, 那么 $d|d', d'|d$:

$$d' = ud, \quad d = vd', \quad d = uvd$$

这样, 若 $d = 0$, d' 也等于零,

$$d = d'$$

若 $d \neq 0$, 我们可以得到 $1 = uv$, u 是一个单位 ε,

$$d' = \varepsilon d$$

证完

从这个定理应用归纳法立刻可以得到

推论 一个唯一分解环 I 的 n 个元 $a_1, a_2, \cdots, a_n$ 在 I 里一定有最大公因子. $a_1, a_2, \cdots, a_n$ 的两个最大公因子只能差一个单位因子.

这样, 若是几个元的某一个最大公因子是一个单位, 这几个元的任何一个最大公因子也是一个单位. 利用这一件事实, 我们可以在一个唯一分解环里规定互素这一个概念.

定义 我们说, 一个唯一分解环的元 $a_1, a_2, \cdots, a_n$ 互素, 假如它们的最大公因子是单位.

这样规定的互素概念显然是普通互素概念的推广.

习　　题

1. 证明本节的推论.

2. 假定在一个唯一分解环里

$$a_1=db_1, a_2=db_2, \cdots, a_n=db_n$$

证明：当而且只当 d 是 $a_1, a_2, \cdots, a_n$ 的一个最大公因子的时候，$b_1, b_2, \cdots, b_n$ 互素.

3. 假定 I 是一个整环，(a) 和 (b) 是 I 的两个主理想. 证明：$(a)=(b)$ 当而且只当 b 是 a 的相伴元的时候.

§3. 主 理 想 环

要知道一个整环是不是一个唯一分解环不是一件容易的事，因为要测验唯一分解定义里的条件(i)，(ii)，或是 Ⅳ，2，定理 2 里的条件(i)，(iii)能否被满足，一般是非常困难的. 以下我们要认识几种特殊的唯一分解环，使得我们在解决以上问题时可以有一点帮助.

第一种是主理想环.

定义　一个整环 I 叫做一个**主理想环**，假如 I 的每一个理想都是一个主理想.

我们说，一个主理想环一定是一个唯一分解环.

为证明这一点，我们需要两个引理. 这两个引理本身也很重要.

引理 1　假定 I 是一个主理想环. 若在序列

$$a_1, a_2, a_3, \cdots \qquad (a_i \in I)$$

里每一个元是前面一个的真因子，那么这个序列一定是一个有限序列.

证明　我们作主理想

$$(a_1), (a_2), (a_3), \cdots$$

由于 a_{i+1} 是 a_i 的因子，显然

$$(a_1) \subset (a_2) \subset (a_3) \cdots$$

我们看这些理想的并集 $\mathfrak{A}$. 我们说，$\mathfrak{A}$ 有以下性质：

(i) 若 $a \in \mathfrak{A}, b \in \mathfrak{A}$，那么 $a-b \in \mathfrak{A}$；

(ii) 若 $a \in \mathfrak{A}, r \in I$，那么 $ra \in \mathfrak{A}$.

因为：由并集的定义，

$$a \in \text{某一个}(a_i), \quad b \in \text{某一个}(a_j)$$

我们可以假定 $i \leqslant j$，那么

$$a \in (a_i) \subset (a_j)$$

a, b 既然都属于理想(a_j)，我们显然有

$$a-b, \ ra \in (a_j) \subset \mathfrak{A}$$

这样，$\mathfrak{A}$ 是 I 的一个理想. 由于 I 是主理想环，$\mathfrak{A}$一定是一个主理想：$\mathfrak{A}=(d)$. 这个 d 属于 $\mathfrak{A}$，所以也属于某一个(a_n). 我们说，这个 a_n 一定是我们的序列里的最后一元. 不然的话，我们还有一个 a_{n+1}. 由于

$$d \in (a_n), \quad a_{n+1} \in (d)$$

可以得到 $$a_n \mid d, \quad d \mid a_{n+1}$$

这就是说 $$a_n \mid a_{n+1}$$

$$a_{n+1} = ca_n$$

但 $$a_{n+1} \mid a_n$$

$$a_n = c' a_{n+1}$$

因而 $$a_{n+1} = cc' a_{n+1}, \quad 1 = cc'$$

c 是一个单位. 这样 a_{n+1} 是 a_n 的相伴元，与 a_{n+1} 是 a_n 的真因子的假定冲突. 证完.

引理 2 假定 I 是一个主理想环，那么 I 的一个素元 p 生成一个最大理想.

证明 假定$\mathfrak{A}$是包含(p)，并且比(p)大的理想．由于I是主理想环，我们有

$$(p)\subset\mathfrak{A}=(a)$$

因而

$$p=ra\quad(r\in I)$$

a是p的因子．但p是素元，所以a不是p的相伴元，就是单位．如果a是p的相伴元：$a=\varepsilon p$，那么

$$a\in(p),(a)=\mathfrak{A}\subset(p)$$

与$\mathfrak{A}$大于(p)的假定不合；所以a只能是单位：$aa^{-1}=1$．这样，

$$1\in(a)=\mathfrak{A},\ \mathfrak{A}=I$$

证完

现在我们证明

定理 一个主理想环I是一个唯一分解环．

证明 我们证明I有IV, 2, 定理2里的性质．

我们看I的一个不是零也不是单位的元a．假定a不能写成有限个素元的乘积，那么a不会是一个素元，所以由IV, 1, 推论，

$$a=bc$$

b和c都是a的真因子．a的这两个真因子之中至少有一个不能写成素元的乘积，不然的话a就会是素元的乘积，与假定冲突．我们得到了结论：假如一个元a没有分解，那么a一定有一个真因子a_1，a_1也没有分解．这样，在元a没有分解的假定之下，我们会得到一个无穷序列

$$a,a_1,a_2,a_3,\cdots$$

在这个序列里每一个元是前面一个的真因子．依照引理1这是不可能的，所以a一定有分解．

假定I的素元p能够整除ab．那么

$$ab=rp\in(p)$$

$$ab\equiv 0\quad((p))$$

这就是说在剩余类环$I/(p)$里，ab所代表的类同0所代表的类

相同：

$$[ab]=[0]=[a][b]$$

依照引理 2，(p)是最大理想，因此依照 III，9，定理，$I/(p)$是一个域．因为域没有零因子，上边的式子告诉我们

$$[a]=[0] \text{ 或 } [b]=[0]$$

这就是说 $a\equiv 0 \quad ((p))$ 或 $b\equiv 0 \quad ((p))$

$$a\in(p) \text{ 或 } b\in(p)$$

这样 $p|a$ 或 $p|b$ 证完

习　　题

1．假定 I 是一个主理想环，并且 $(a,b)=(d)$．证明：d 是 a 和 b 的一个最大公因子，因此 a 和 b 的任何最大公因子 d' 都可以写成以下形式：

$$d'=sa+tb \qquad (s,t\in I)$$

2．一个主理想环的每一个最大理想都是由一个素元所生成的．

3．我们看两个主理想环 I 和 I_0，I_0 是 I 的子环．假定 a 和 b 是 I_0 的两个元，d 是这两个元在 I_0 里的一个最大公因子．证明：d 也是这两个元在 I 里的一个最大公因子．

§4．欧 氏 环

我们要认识的第二种唯一分解环叫做欧氏环．

定义　一个整环 I 叫做一个欧氏环，假如

（i）有一个从 I 的非零元所作成的集合到 $\geqslant 0$ 的整数集合的映射 ϕ 存在；

（ii）给定了 I 的一个不等于零的元 a，I 的任何元 b 都可以写成

$$b=qa+r \quad (q,r\in I)$$

的形式，这里或是 $r=0$ 或是 $\phi(r)<\phi(a)$．

例 整数环是一个欧氏环. 因为:

ϕ: $a \longrightarrow |a| = \phi(a)$ ($|a|$表示整数 a 的绝对值)

是一个适合条件 (i) 的映射. 给了整数 $a \neq 0$, 任何整数 b 是可以写成

$$b = qa + r$$

的形式, 这里 $r = 0$ 或 $\phi(r) = |r| < |a| = \phi(a)$.

我们有

定理 1 任何欧氏环 I 一定是一个主理想环, 因而一定是一个唯一分解环.

证明 我们看 I 的一个理想 $\mathfrak{A}$.

若是 $\mathfrak{A}$ 只包含零元, 那么 $\mathfrak{A} = (0)$, $\mathfrak{A}$ 是一个主理想.

假定 $\mathfrak{A}$ 包含不等于零的元. 由欧氏环的定义, 存在一个映射 ϕ, 在这个映射之下 $\mathfrak{A}$ 的每一个不等于零的元 x 有一个象 $\phi(x)$, 并且这些 $\phi(x)$ 都是 $\geqslant 0$ 的整数. 在这些 $\geqslant 0$ 的整数之中一定有一个最小的, 因此我们可以找到 $\mathfrak{A}$ 的一个不等于零的元 a, 使得对于 $\mathfrak{A}$ 的任何不等于零的元 x 来说, 都有

$$\phi(a) \leqslant \phi(x)$$

再一次由欧氏环的定义, $\mathfrak{A}$ 的每一个元 b 都可以写成

$$b = qa + r$$

的形式, 这里

$$r = 0 \text{ 或 } \phi(r) < \phi(a)$$

因为 a 和 b 都属于 $\mathfrak{A}$,

$$r = b - qa$$

也属于 $\mathfrak{A}$. 若是 $r \neq 0$, 那么 $\mathfrak{A}$ 有一个不等于零的元 r, 适合条件

$$\phi(r) < \phi(a)$$

与 a 的取法不合. 这样,

$$r = 0, \quad b = qa, \quad \mathfrak{A} = (a)$$

证完

由于上面的例同这个定理我们立刻有

定理 2 整数环是一个主理想环，因而是一个唯一分解环.

另一种常见的欧氏环就是一个域上的多项式环. 我们先证明一个

引理 假定 $I[x]$ 是整环 I 上的一元多项式环，$I[x]$ 的元

$$g(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

的最高系数 a_n 是 I 的一个单位. 那么 $I[x]$ 的任意多项式 $f(x)$ 都可以写成

$$f(x)=q(x)g(x)+r(x)\quad (q(x),r(x)\in I[x])$$

的形式，这里或是 $r(x)=0$ 或是 $r(x)$ 的次数小于 $g(x)$ 的次数 n.

证明 若是 $f(x)=0$ 或是 $f(x)$ 的次数小于 n，那么我们取 $q(x)=0$, $r(x)=f(x)$ 就行了. 假定

$$f(x)=b_mx^m+\cdots+b_0\quad (m\geqslant n)$$

我们取
$$q_1(x)=a_n^{-1}b_mx^{m-n}$$

那么

$$f(x)-q_1(x)g(x)=b_mx^m+\cdots+b_0-(b_mx^m+a_n^{-1}b_ma_{n-1}x^{m-1}+\cdots)$$
$$=f_1(x)$$

$f_1(x)=0$ 或 $f_1(x)$ 的次数小于 m. 假如 $f_1(x)=0$ 或是 $f_1(x)$ 的次数已经小于 n，那么取 $q(x)=q_1(x)$ 就行了. 假如 $f_1(x)$ 的次数还大于 n，用同样的方法我们可以得到

$$f_1(x)-q_2(x)g(x)=f(x)-[q_1(x)+q_2(x)]g(x)=f_2(x)$$

$f_2(x)=0$ 或是 $f_2(x)$ 的次数小于 $m-1$. 这样下去，我们总可以得到

$$f(x)=[q_1(x)+q_2(x)+\cdots+q_i(x)]g(x)+f_i(x)$$

$f_i(x)=0$ 或是 $f_i(x)$ 的次数小于 n. 证完.

由这个引理我们很容易证明

定理 3 一个域 F 上的一元多项式环 $F[x]$ 是一个欧氏环.

证明 利用多项式的次数我们显然可以规定一个合于条件(i)的映射，就是

ϕ: $f(x) \longrightarrow f(x)$的次数

假定 $g(x) \in F[x]$, $g(x) \neq 0$, 那么 $g(x)$ 的最高系数 $a_n \neq 0$. 但 a_n 属于域 F, 域的每一个不等于零的元都是一个单位，所以由引理，每一个 $F[x]$的 $f(x)$都可以写成

$$f(x)=q(x)g(x)+r(x)$$

的形式，这里 $r(x)=0$ 或是 $r(x)$的次数$<g(x)$的次数. 证完.

注意 以上两节的结果只是说一个欧氏环一定是一个主理想环，一个主理想环一定是一个唯一分解环. 但是反过来一个唯一分解环未必是一个主理想环，一个主理想环也未必是一个欧氏环. 一个唯一分解环不是一个主理想环的例子我们在下一节就可以看到. 一个主理想环不是一个欧氏环的例子我们不能引用到本书里来，读者可以参看：Motzkin, The Euclidean algorithm, Bull. Amer. Math. Soc. 55, p. p. 1142—1146, (1949).

习 题

1. 证明，一个域一定是一个欧氏环.

2. 我们看有理数域 F 上的一元多项式环 $F[x]$. 理想

$$(x^2+1, x^5+x^3+1)$$

等于怎样的一个主理想？

3. 证明由所有复数 $a+bi$(a, b 是整数)所作成的环是一个欧氏环（取 $\phi(a)=|a|^2$).

§5. 多项式环的因子分解

我们已经看到，一个域 F 上的一元多项式环 $F[x]$是唯一分解环. 多项式环的因子分解在代数里占一个特别重要的地位，我们

在这一节里要专门把这个问题讨论一下.

我们将要得到的结果是：一个唯一分解环 I 上的多元多项式环 $I[x_1, x_2, \cdots, x_n]$ 本身也是唯一分解环.

以下我们依照普通习惯，把一个素多项式叫做不可约多项式，把一个有真因子的多项式叫做可约多项式.

我们先讨论唯一分解环 I 上的一元多项式环 $I[x]$.

首先我们有以下简单事实：

(A) I 的单位是 $I[x]$ 的仅有的单位.

因为：I 的单位都是 $I[x]$ 的单位，显然. 另一方面，若 $f(x)$ 是 $I[x]$ 的单位，

$$f(x)g(x)=1 \quad (g(x)\in I[x])$$

那么由多项式的乘法定义，$f(x)$ 同 $g(x)$ 的次数都等于零. 这就是说，$f(x), g(x)\in I$，$f(x)$ 是 I 的单位.

在以下的讨论里我们需要一个新的概念. 假定

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

是 $I[x]$ 的一个多项式. 那么由于 I 是唯一分解环，$f(x)$ 的系数 $a_0, a_1, \cdots, a_n$ 在 I 里有最大公因子.

定义 $I[x]$ 的一个元 $f(x)$ 叫做一个**本原多项式**，假如 $f(x)$ 的系数的最大公因子是单位.

按照这个定义，显然：

(B) 一个本原多项式不会等于零.

(C) 若本原多项式 $f(x)$ 可约，那么

$$f(x)=g(x)h(x)$$

这里 $g(x)$ 和 $h(x)$ 的次数都大于零，因而都小于 $f(x)$ 的次数.

本原多项式在我们的讨论里占一个很重要的地位. 我们证明重要的

引理 1 假定 $f(x)=g(x)h(x)$. 那么 $f(x)$ 是本原多项式，当

而且只当 $g(x)$ 和 $h(x)$ 都是本原多项式的时候.

证明 若是 $f(x)$ 是本原多项式，显然 $g(x)$ 和 $h(x)$ 也都是本原多项式.

现在假定

$$g(x)=a_0+a_1x+\cdots$$

$$h(x)=b_0+b_1x+\cdots$$

是两个本原多项式. 如果

$$f(x)=g(x)h(x)=c_0+c_1x+\cdots$$

不是本原多项式，那么 $c_0, c_1, \cdots$ 有一个最大公因子 d，d 不是 I 的单位. 由于(B)，$g(x)\neq 0, h(x)\neq 0$，因而 $f(x)\neq 0, d\neq 0$. 这样，由于 I 是唯一分解环，有一个 I 的素元 p 可以整除 d，因而可以整除每一个 c_k. 这个 p 不能整除所有的 a_i，也不能整除所有的 b_j，不然 $g(x)$ 和 $h(x)$ 不会是本原多项式. 假定 a_r 和 b_s 各是 $g(x)$ 和 $h(x)$ 的头一个不能被 p 整除的系数. $f(x)$ 的系数 c_{r+s} 可以写成以下形式

$$c_{r+s}=a_rb_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\cdots$$

$$+a_{r-1}b_{s+1}+a_{r-2}b_{s+2}+\cdots$$

在这个式子里除了 a_rb_s 以外，每项都能被 p 整除，所以 a_rb_s 也能被 p 整除，因而由于 I 是唯一分解环，a_r 或 b_s 能被 p 整除，与这两个元的取法相反. 这样 $f(x)$ 必须是本原多项式. 证完.

现在我们用 I 的商域 Q 来作 Q 上的一元多项式环 $Q[x]$，那么 $Q[x]$ 包含 $I[x]$. 我们知道 $Q[x]$ 是唯一分解环，我们要由这一件事实来证明 $I[x]$ 也是唯一分解环.

引理 2 $Q[x]$ 的每一个不等于零的多项式 $f(x)$ 都可以写成

$$f(x)=\frac{b}{a}f_0(x)$$

的样子，这里 $a, b\in I$，$f_0(x)$ 是 $I[x]$ 的本原多项式. 若是 $g_0(x)$ 也有

$f_0(x)$的性质，那么

$$g_0(x)=\varepsilon f_0(x) \quad (\varepsilon \text{ 是 } I \text{ 的单位})$$

证明 Q的元都可以写成 $\frac{b}{a}(a,b\in I,a\neq 0)$的样子，因此

$$f(x)=\frac{b_0}{a_0}+\frac{b_1}{a_1}x+\cdots+\frac{b_n}{a_n}x^n \quad (a_i,b_i\in I)$$

叫 $a=a_0a_1\cdots a_n$，那么

$$f(x)=\frac{1}{a}(c_0+c_1x+\cdots+c_nx^n) \quad (c_i\in I)$$

叫 b 是 $c_0,c_1,\cdots,c_n$的一个最大公因子，那么

$$f(x)=\frac{b}{a}f_0(x)$$

$f_0(x)$是本原多项式(Ⅳ,2，习题 2)．假定另一方面

$$f(x)=\frac{d}{c}g_0(x)$$

$c,d\in I$，$g_0(x)$是 $I[x]$的本原多项式．那么

$$h(x)=bcf_0(x)=adg_0(x)$$

是 $I[x]$的一个多项式．由于 $f_0(x)$和 $g_0(x)$都是本原多项式，bc 和 ad 一定同是 $h(x)$的系数的最大公因子(Ⅳ,2，习题 2)，因而

$$bc=\varepsilon ad \quad (\varepsilon \text{ 是 } I \text{ 的单位})$$

这样
$$\varepsilon f_0(x)=g_0(x)$$
证完

引理 3 $I[x]$的一个本原多项式 $f_0(x)$在 $I[x]$里可约的充分而且必要条件是：$f_0(x)$在 $Q[x]$里可约．

证明 假定 $f_0(x)$在 $Q[x]$里可约．这时，因为 $f_0(x)$ 显然也是 $Q[x]$的本原多项式，由(C)，

$$f_0(x)=g(x)h(x)$$

$g(x)$和 $h(x)$都属于 $Q[x]$，并且它们的次数都大于零．由引理 2，

$$f_0(x)=\frac{b}{a}g_0(x)\frac{b'}{a'}h_0(x)=\frac{b}{a}\,\frac{b'}{a'}g_0(x)h_0(x)$$

$a,b,a',b'\in I$，$g_0(x)$和$h_0(x)$都是$I[x]$的本原多项式．由引理1，$g_0(x)h_0(x)$还是本原多项式；由引理2，

$$f_0(x)=\varepsilon g_0(x)\,h_0(x) \qquad (\varepsilon\text{ 是 } I \text{ 的单位})$$

因此 $$\varepsilon g_0(x),h_0(x)\in I[x]$$

但$\varepsilon g_0(x)$和$h_0(x)$的次数各等于$g(x)$和$h(x)$的次数，因而都大于零：$\varepsilon g_0(x)$，$h_0(x)\bar{\in}I$；由(A)，$\varepsilon g_0(x)$和$h_0(x)$都不是$I[x]$的单位．这样，由Ⅳ，1，定理3，$f_0(x)$在$I[x]$里可约．

假定$f_0(x)$在$I[x]$里可约．这时，由(C)，

$$f_0(x)=g(x)h(x)$$

$g(x)$和$h(x)$都属于$I[x]$，并且它们的次数都大于零．这样，由(A)，把$g(x)$和$h(x)$看作$Q[x]$的元，这两个多项式也不是$Q[x]$的单位；由Ⅳ，1，定理3，$f_0(x)$在$Q[x]$里可约．证完．

引理4 $I[x]$的一个次数大于零的本原多项式$f_0(x)$在$I[x]$里有唯一分解．

证明 我们先证明$f_0(x)$可以写成不可约多项式的乘积．若是$f_0(x)$本身不可约，我们用不着再证明什么．假定$f_0(x)$可约．由(C)和引理1，

$$f_0(x)=g_0(x)h_0(x)$$

$g_0(x)$和$h_0(x)$都是本原多项式，并且它们的次数都小于$f_0(x)$的次数．这样，假如$g_0(x)$和$h_0(x)$还是可约，我们又可以把它们写成次数更小的本原多项式的乘积．由于$f_0(x)$的次数是有限正整数，最后我们可以得到

$$(1) \qquad f_0(x)=p_0^{(1)}(x)p_0^{(2)}(x)\cdots p_0^{(r)}(x)$$

$p_0^{(i)}(x)$是不可约本原多项式．

假定$f_0(x)$还有一种分解

$$(2) \qquad f_0(x)=q_0^{(1)}(x)q_0^{(2)}(x)\cdots q_0^{(s)}(x)$$

那么由引理1，$q_0^{(i)}(x)$是不可约本原多项式．由引理3，$p_0^{(i)}(x)$和

$q_0^{(i)}(x)$在$Q[x]$里还是不可约，这就是说，(1) 和(2)也是$f_0(x)$在$Q[x]$里的两种分解. 但$Q[x]$是唯一分解环,所以我们有

$$r=t$$

并且由(A)，我们可以假定

$$q_0^{(i)}(x)=\frac{b_i}{a_i}p_0^{(i)}(x) \qquad (a_i, b_i\in I)$$

这样，由引理 2，

$$q_0^{(i)}(x)=\varepsilon_i p_0^{(i)}(x) \quad (\varepsilon_i \text{ 是 } I \text{ 的单位})$$

$f_0(x)$在 $I[x]$里有唯一分解. 证完.

现在我们可以证明

定理 1 若是 I 是唯一分解环，那么 $I[x]$也是.

证明 我们看 $I[x]$的一个不是零也不是单位的多项式 $f(x)$. 若 $f(x)\in I$, 那么由于 I 是唯一分解环，$f(x)$显然有唯一分解. 若 $f(x)$是本原多项式，由引理 4, $f(x)$也有唯一分解. 这样，我们只需看

$$f(x)=d\,f_0(x)$$

d 不是 I 的单位，$f_0(x)$是次数大于零的本原多项式时的情形.

这时，因 d 有分解

$$d=p_1p_2\cdots p_m \qquad (p_i \text{ 是 } I \text{ 的素元})$$

$f_0(x)$有分解

$$f_0(x)=p_0^{(1)}(x)p_0^{(2)}(x)\cdots p_0^{(r)}(x)$$

$p_0^{(i)}(x)$是不可约本原多项式，所以 $f(x)$在 $I[x]$里有分解：

$$f(x)=p_1p_2\cdots p_m p_0^{(1)}(x)p_0^{(2)}(x)\cdots p_0^{(r)}(x)$$

假定 $f(x)$在 $I[x]$里有另一种分解：

$$f(x)=q_1q_2\cdots q_n q_0^{(1)}(x)q_0^{(2)}(x)\cdots q_0^{(t)}(x)$$

$q_i\in I$, $q_0^{(i)}(x)\bar{\in} I$, q_i, $q_0^{(i)}(x)$都是 $I[x]$的不可约多项式. 这时，q_i 一定是 I 的素元，$q_0^{(i)}(x)$一定是不可约本原多项式. 因为：q_i 若不是

I 的素元，显然也不会是 $I[x]$ 的不可约多项式；$q_0^{(i)}(x)$ 若不是本原多项式，它的系数的最大公因子 d_i 显然是它的一个真因子，因而 $q_0^{(i)}(x)$ 也不会是不可约多项式．这样由引理 1 和 2，我们有

(3) $$f_0(x)=p_0^{(1)}(x)\cdots p_0^{(r)}(x)=[\varepsilon q_0^{(1)}(x)]q_0^{(2)}(x)\cdots q_0^{(t)}(x)$$

ε 是 I 的单位；因而

(4) $$d=p_1p_2\cdots p_m=[\varepsilon^{-1}q_1]q_2\cdots q_n$$

(3)式表示的是本原多项式 $f_0(x)$ 的两种分解，因而由引理 4，

$$t=r$$

而且我们可以假定

$$q_0^{(i)}(x)=\varepsilon_i p_0^{(i)}(x)\qquad(\varepsilon_i \text{ 是 } I \text{ 的单位})$$

(4)表示的是唯一分解环 I 的元 d 的两种分解，因而

$$n=m$$

而且我们可以假定

$$q_i=\varepsilon_i' p_i\qquad(\varepsilon_i' \text{ 是 } I \text{ 的单位})$$

这样，$I[x]$ 是唯一分解环．证完．

由定理 1，应用归纳法立刻可以得到

定理 2 若 I 是唯一分解环，那么 $I[x_1,x_2,\cdots,x_n]$ 也是，这里 $x_1,x_2,\cdots,x_n$ 是 I 上的无关未定元．

由定理 1，当 I 是整数环的时候，$I[x]$ 是一个唯一分解环．但我们知道，这个多项式环不是一个主理想环(Ⅲ，7，例 3)．这样，我们有了一个唯一分解环不是主理想环的例子．

习　题

1．假定 I 是一个唯一分解环，Q 是 I 的商域．证明，$I[x]$ 的一个多项式若是在 $Q[x]$ 里可约，它在 $I[x]$ 里已经可约．

2．假定 $I[x]$ 是整环 I 上的一元多项式环．$f(x)$ 属于 $I[x]$ 但不属于 I，并且 $f(x)$ 的最高系数是 I 的一个单位．证明 $f(x)$ 在 $I[x]$ 里有分解．

§6. 因子分解与多项式的根

在这一章的最后我们讨论一下，一个整环 I 上的一元多项式环 $I[x]$ 里的因子分解同多项式的根的关系. 这一节的结果都是中学代数的习知定理的推广.

我们先下

定义 I 的元 a 叫做 $I[x]$ 的**多项式** $f(x)$ **的一个根**，假如 $f(a)=0$.

我们有

定理 1 a 是 $f(x)$ 的一个根，当而且只当 $f(x)$ 能被 $x-a$ 整除的时候.

证明 假定 $x-a$ 能够整除 $f(x)$,

$$f(x)=(x-a)g(x)$$

那么由 Ⅲ,6,定理 3,

$$f(a)=(a-a)g(a)=0$$

a 是 $f(x)$ 的根.

反过来假定 a 是 $f(x)$ 的根. 因为 $x-a$ 的最高系数 1 是一个单位,依照 Ⅳ,4,引理,

$$f(x)=q(x)(x-a)+r,\quad r\in I$$

用 a 代入,得 $\quad f(a)=q(a)(a-a)+r$

但由根的定义,$f(a)=0$,所以

$$0=r$$

$$f(x)=q(x)(x-a)$$

$x-a$ 能够整除 $f(x)$. 证完.

定理 2 I 的 k 个不同的元 $a_1,a_2,\cdots,a_k$ 都是 $f(x)$ 的根,当而且只当 $f(x)$ 能被 $(x-a_1)(x-a_2)\cdots(x-a_k)$ 整除的时候.

证明 $f(x)$若是能够被$(x-a_1)(x-a_2)\cdots(x-a_k)$整除，显然$a_1,a_2,\cdots,a_k$都是$f(x)$的根.

现在假定$a_1,a_2,\cdots,a_k$都是$f(x)$的根. 由定理1,

$$f(x)=(x-a_1)f_1(x)$$

用a_2代入,得
$$0=(a_2-a_1)f_1(a_2)$$
但$a_2-a_1\neq 0$, I又没有零因子，所以$f_1(a_2)=0$，a_2是$f_1(x)$的根.因此

$$f_1(x)=(x-a_2)f_2(x)$$
$$f(x)=(x-a_1)(x-a_2)f_2(x)$$

这样下去,得到

$$f(x)=(x-a_1)(x-a_2)\cdots(x-a_k)f_k(x)$$

证完

推论 若$f(x)$的次数是n，那么$f(x)$在I里至多有n个根.

根据定理2,我们下

定义 I的元a叫做$f(x)$的一个**重根**,假如$f(x)$能被$(x-a)^k$整除,k是大于1的整数.

关于重根我们有一个类似定理1的定理，不过在这里我们需要导数这一个概念.

定义 由多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

唯一决定的多项式

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$$

叫做$f(x)$的**导数**.

导数适合以下计算规则:

$$[f(x)+g(x)]'=f'(x)+g'(x)$$
$$[f(x)g(x)]'=f(x)g'(x)+g(x)f'(x)$$
$$[f(x)^t]'=tf(x)^{t-1}f'(x)$$

这几个公式可以由以上定义纯代数地算出来，这一点我们不

证明了.

定理 3　$f(x)$的一个根 a 是一个重根,当而且只当 $f'(x)$能被 $x-a$ 整除的时候.

证明　假定 a 是 $f(x)$的重根,那么

$$f(x)=(x-a)^k g(x) \qquad (k>1)$$

$$f'(x)=(x-a)^k g'(x)+k(x-a)^{k-1}g(x)$$

$$=(x-a)^{k-1}[(x-a)g'(x)+kg(x)]$$

$f'(x)$能够被$(x-a)$整除.

假定 a 不是 $f(x)$的重根,那么

$$f(x)=(x-a)g(x),\quad (x-a)\nmid g(x)$$

$$f'(x)=(x-a)g'(x)+g(x)$$

$$f'(a)=g(a)\neq 0$$

$f'(x)$不能被$(x-a)$整除. 证完.

推论　假定 $I[x]$ 是一个唯一分解环. I 的元 a 是 $f(x)$的一个重根的充分而且必要条件是: $x-a$ 能整除 $f(x)$和 $f'(x)$的最大公因子.

习　　题

1. 假定 R 是模 16 的剩余类环. $R[x]$的多项式 x^2 在 R 里有多少个根?

2. 假定 F 是模 3 的剩余类环, 我们看 $F[x]$ 的多项式 $f(x)=x^3-x$. 证明, $f(a)=0$, 不管 a 是 F 的哪一个元.

3. 证明本节的导数计算规则.

第五章　扩　　域

在这一章里我们要对于域作一些进一步的讨论．我们不准备证明一些复杂的结构定理，而主要是对单扩域、代数扩域、多项式的分裂域、有限域和可离扩域作一些讨论．

§1．扩域、素域

我们先说明一下，研究域所用的方法．

定义　一个域E叫做一个域F的扩域（扩张），假如F是E的子域．

我们知道，实数域是在它的子域有理数域上建立起来的，而复数域是在它的子域实数域上建立起来的．研究域的方法就是：从一个给定的域F出发，来研究它的扩域．

这就有如何选择域F的问题．我们有以下事实．

定理1　令E是一个域．若E的特征是∞，那么E含有一个与有理数域同构的子域；若E的特征是素数p，那么E含有一个与$R/(p)$同构的子域，这里R是整数环，(p)是由p生成的主理想．

证明　域E包含一个单位元e．因此E也包含所有ne（n是整数）．令R'是所有ne作成的集合．那么

$$\phi: \qquad n \longrightarrow ne$$

显然是整数环R到R'的一个同态满射．

情形1．E的特征是∞．这时ϕ是一个同构映射：

$$R \cong R'$$

但E包含R'的商域F'．由Ⅲ，10，定理4，F'与R的商域，也就是

有理数域同构.

情形 2. E 的特征是素数 p. 这时

$$R/\mathfrak{A}\cong R'$$

此处 $\mathfrak{A}$ 是 ϕ 的核. 但

$$p\dashrightarrow pe=0$$

所以 $\mathfrak{A}\ni p$, 因而 $\mathfrak{A}\supset(p)$. 由 [IV, 3, 引理 2, (p) 是一个最大理想. 另一方面,

$$1\longrightarrow e\neq 0$$

所以 $\mathfrak{A}\neq R$ 而 $\mathfrak{A}=(p)$, 因而

$$R/(p)\cong R'$$

证完

有理数域和 $R/(p)$ 显然都不含真子域.

定义 一个域叫做一个**素域**, 假如它不含真子域.

由定理 1 知道: 一个素域或是与有理数域同构, 或是与 $R/(p)$ 同构. 因此定理 1 的另一形式是

定理 2 令 E 是一个域. 若 E 的特征是 ∞, 那么 E 包含一个与有理数域同构的素域; 若 E 的特征是素数 p, 那么 E 包含一个与 $R/(p)$ 同构的素域.

由定理 2, 一个任意域都是一个素域的扩域; 因此, 如果我们能够决定素域的所有扩域, 我们就掌握了所有的域. 但事实上研究素域的扩域并不比研究一个任意域的扩域来得容易. 因此我们研究域的普通方法是: 设法决定一个任意域 F 的所有扩域 E.

现在我们极粗略地描述一下一个扩域的结构.

令 E 是域 F 的一个扩域. 我们从 E 里取出一个子集 S 来. 我们用 $F(S)$ 表示含 F 和 S 的 E 的最小子域, 把它叫做添加集合 S 于 F 所得的扩域.

$F(S)$ 的存在容易看出. 因为, E 的确有含 F 和 S 的子域, 例如 E 本身. 一切这样的子域的交集显然是含 F 和 S 的 E 的最小子域.

更具体地说，$F(S)$刚好包含E的一切可以写成

(1) $$\frac{f_1(\alpha_1, \alpha_2, \cdots, \alpha_n)}{f_2(\alpha_1, \alpha_2, \cdots, \alpha_n)}$$

形式的元，这里$\alpha_1, \alpha_2, \cdots, \alpha_n$是$S$中的任意有限个元素，而$f_1$和$f_2(\neq 0)$是$F$上的这些$\alpha$的多项式．这是因为：$F(S)$既然是含有$F$和$S$的一个域，它必然含有一切可以写成形式(1)的元；另一方面，一切可以写成形式(1)的元已经作成一个含有F和S的域．

适当选择S，我们可以使$E=F(S)$．例如，取$S=E$，就可以作到这一点．实际上，为了作到这一点，常常只须取E的一个真子集S．

现在假定$E=F(S)$．那么按照上面的分析，E是一切添加S的有限子集于F所得子域的并集．这样，求E就归结为求添加有限集于F所得的子域以及求这些子域的并集．

若S是一个有限集：$S=\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$，那么我们也把$F(S)$记作

$$F(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

叫做添加元素$\alpha_1, \alpha_2, \cdots, \alpha_n$于$F$所得的子域．

为了便于讨论添加有限个元素所得的子域，我们证明下述的一般定理．

定理 3 令E是域F的一个扩域，而S_1和S_2是E的两个子集．那么

$$F(S_1)(S_2)=F(S_1 \cup S_2)=F(S_2)(S_1)$$

证明 $F(S_1)(S_2)$是一个包含F、S_1和S_2的E的子域，而$F(S_1 \cup S_2)$是包含F和$S_1 \cup S_2$的E的最小子域．因此

(2) $$F(S_1)(S_2) \supset F(S_1 \cup S_2)$$

另一方面，$F(S_1 \cup S_2)$是一个包含F、S_1和S_2，因而是一个包含$F(S_1)$和S_2的E的子域．但$F(S_1)(S_2)$是包含$F(S_1)$和S_2的E

的最小子域，因此

(3) $$F(S_1)(S_2)\subset F(S_1\cup S_2)$$

由(2)和(3)，得

$$F(S_1)(S_2)=F(S_1\cup S_2)$$

同样可以得到

$$F(S_2)(S_1)=F(S_1\cup S_2)$$ 证完

根据定理3，我们可以把添加一个有限集归结为陆续添加单个的元素，例如

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$$

定义 添加一个元素 α 于域 F 所得的扩域 $F(\alpha)$ 叫做域 F 的一个**单扩域**(扩张).

单扩域是最简单的扩域. 我们在下一节将先讨论这种扩域的结构.

习 题

证明：$F(S)$的一切添加S的有限子集于F所得的子域的并集是一个域.

§2. 单 扩 域

假定 E 是域 F 的扩域，而 α 是 E 的一个元.

要讨论单扩域 $F(\alpha)$的结构，我们把 E 的元分成两类.

定义 α 叫做域 F 上的一个**代数元**，假如存在 F 的不都等于零的元 $a_0,a_1,\cdots,a_n$, 使得

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0$$

假如这样的 $a_0,a_1,\cdots,a_n$ 不存在，α 就叫做 F 上的一个**超越元**. 若 α 是 F 上的一个代做元，$F(\alpha)$就叫做 F 的一个**单代数扩域**；若 α 是 F 上的一个超越元，$F(\alpha)$就叫做 F 的一个**单超越扩域**.

单扩域的结构通过以下定理可以掌握.

定理 1　若 α 是 F 上的一个超越元,那么

$$F(\alpha)\cong F[x]\text{的商域}$$

这里 $F[x]$ 是 F 上的一个未定元 x 的多项式环.

若 α 是 F 上的一个代数元,那么

$$F(\alpha)\cong F[x]/(p(x))$$

这里 $p(x)$ 是 $F[x]$ 的一个唯一确定的、最高系数为 1 的不可约多项式,并且 $p(\alpha)=0$.

证明　$F(\alpha)$ 包含 F 上的 α 的多项式环

$$F[\alpha]=\{\text{一切}\sum a_k\alpha^k,\ a_k\in F\}$$

我们知道,

$$\sum a_kx^k\longrightarrow\sum a_k\alpha^k$$

是 F 上的未定元 x 的多项式环 $F[x]$ 到 $F[\alpha]$ 的同态满射. 现在我们分两个情形来看.

情形 1. α 是 F 上的超越元. 这时以上映射是同构映射:

$$F[\alpha]\cong F[x]$$

由 Ⅱ, 10, 定理 4,

$$F[\alpha]\text{的商域}\cong F[x]\text{的商域}$$

由 Ⅱ, 10, 定理 3, 我们可以知道,

$$(1)\qquad F[\alpha]\text{的商域}\subset F(\alpha)$$

另一方面, $F[\alpha]$ 的商域包含 F 也包含 α, 因此, 由 $F(\alpha)$ 的定义

$$(2)\qquad F(\alpha)\subset F[\alpha]\text{的商域}$$

由(1)和(2)得

$$F(\alpha)=F[\alpha]\text{的商域}$$

因而

$$F(\alpha)\cong F[x]\text{的商域}$$

情形 2. α 是 F 上的代数元. 这时

$$F[\alpha]\cong F[x]/\mathfrak{A}$$

这里 $\mathfrak{A}$ 是上述同态满射的核．由 IV, 4, 定理 3 和定理 1，$F[x]$是一个主理想环，所以

$$\mathfrak{A}=(p(x))$$

$F[x]$的一个主理想的两个生成元能够互相整除，因而它们只能差一个单位因子，而 $F[x]$的单位就是 F 的非零元．所以令 $p(x)$的最高系数是 1, $p(x)$就是唯一确定的．由 $\mathfrak{A}$ 的定义得: $p(\alpha)=0$; 由此得 $p(x)$不是 F 的非零元．但 α 是 F 上的代数元，所以 $p(x)$也不是零多项式．因此，$p(x)$的次数$\geqslant 1$.

我们说，$p(x)$是 $F[x]$的一个不可约多项式．不然的话，将有

$$p(x)=g(x)h(x),\quad g(x)\text{ 和 }h(x)\text{ 的次数}<p(x)\text{ 的次数}$$

从而得
$$p(\alpha)=g(\alpha)h(\alpha)=0$$

但 $g(\alpha)$和 $h(\alpha)$都是域 $F(\alpha)$的元，而域没有零因子，所以由上式可以得到

$$g(\alpha)=0\ \text{ 或 }\ h(\alpha)=0$$

这就是说，$g(x)\in\mathfrak{A}$ 或 $h(x)\in\mathfrak{A}$，即

$$p(x)\mid g(x)\ \text{ 或 }\ p(x)\mid h(x)$$

这是一个矛盾．

这样，$p(x)$是一个不可约多项式，因而$(p(x))$是 $F[x]$的一个最大理想，而 $F[x]/(p(x))$是一个域．这样，$F[\alpha]$是一个域．但 $F[\alpha]$ 包含 F 也包含 α, 并且 $F[\alpha]\subset F(\alpha)$，所以

$$F(\alpha)=F[\alpha]\cong F[x]/(p(x))$$ 证完

以上定理把单扩域归结到我们已经知道的域．当 α 是域 F 上代数元的时候，我们还可以把 $F(\alpha)$描述得更清楚一点．

定理 2　令 α 是域 F 上的一个代数元，并且

$$F(\alpha)\cong F[x]/(p(x))$$

那么 $F(\alpha)$的每一个元都可以唯一地表成

$$\sum_{i=0}^{n-1} a_i \alpha^i \quad (a_i \in F)$$

的形式，这里 n 是 $p(x)$ 的次数．要把这样的两个多项式 $f(\alpha)$ 和 $g(\alpha)$ 相加，只需把相当的系数相加；$f(\alpha)$ 与 $g(\alpha)$ 的乘积等于 $r(\alpha)$，这里 $r(x)$ 是用 $p(x)$ 除 $f(x)g(x)$ 所得的余式．

证明 由于 $F(\alpha)=F[\alpha]$，所以 $F(\alpha)$ 的一个任意元 β 可以写成

$$\beta = h(\alpha) = \sum b_i \alpha^i \quad (b_i \in F)$$

的形式．但

$$h(x) = q(x)p(x) + r(x)$$

其中

$$r(x) = \sum_{i=0}^{n-1} a_i x^i \quad (a_i \in F)$$

因而，由于 $p(\alpha)=0$，有

$$\beta = h(\alpha) = r(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i$$

这种表示法是唯一的．因为：假如

$$\beta = r_1(\alpha) = r_2(\alpha),\quad r_1(x) \text{和} r_2(x) \text{的次数} < n$$

那么

$$r_1(\alpha) - r_2(\alpha) = k(\alpha) = 0$$
$$p(x) \mid k(x)$$

由于 $k(x)$ 的次数 $<n$，得

$$k(x)=0,\quad r_1(x)=r_2(x)$$

由以上证明可以看出，定理的后一部分成立．证完．

我们已经看到，多项式 $p(x)$ 对于一个单代数扩域的重要性．$p(x)$ 显然是理想 $\mathfrak{A}$ 里的一个次数最低的多项式．

定义 $F(x)$中满足条件 $p(\alpha)=0$ 的次数最低的多项式

$$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$$

叫做元 α 的在 F 上的**极小多项式**. n 叫做 α 的在 F 上的**次数**.

以上的讨论是在域 F 有扩域 E 的前提下进行的. 现在我们问,若是只给了一个域 F,是不是有 F 的单扩域存在?

存在 F 的单超越扩域容易看出. 我们知道, F 上的一个未定元 x 的多项式环 $F[x]$ 和 $F[x]$的商域都是存在的. $F[x]$的商域显然是包含 F 和 x 的最小域,而按照未定元的定义, x 是 F 上的一个超越元. 因此 $F[x]$的商域就是 F 的一个单超越扩域. 由定理 1, F 的任何单超越扩域都是同构的.

现在我们证明

定理 3 对于任一给定域 F 以及 F 上一元多项式环 $F[x]$的给定不可约多项式

$$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$$

总存在 F 的单代数扩域 $F(\alpha)$, 其中 α 在 F 上的极小多项式是 $p(x)$.

证明 有了 F 和 $p(x)$,我们可以作剩余类环

$$K'=F[x]/(p(x))$$

因为 $p(x)$是不可约多项式,所以$(p(x))$是一个最大理想, 因而 K' 是一个域.

我们知道,有 $F[x]$到 K' 的同态满射

$$f(x)\longrightarrow\overline{f(x)}$$

这里$\overline{f(x)}$是 $f(x)$所在的剩余类. 由于 $F\subset F[x]$, 在这个同态满射之下, F 有一个象$\overline{F}\subset K'$,并且 F 与 $\overline{F}$ 同态. 但对于 F 的元 a 和 b 来说,

$$a\neq b\Longrightarrow p(x)\nmid a-b,\ \overline{a-b}\neq\bar{0}\Longrightarrow\bar{a}\neq\bar{b}$$

所以 F 与 $\overline{F}$ 同构. 这样,由于 K' 和 F 没有共同元,根据 Ⅲ,5,定理

4，我们可以把 K' 的子集 $\bar{F}$ 用 F 来掉换，而得到一个域 K，使得

$$K \cong K', \quad F \subset K$$

现在我们看 $F[x]$ 的元 x 在 K' 里的象 $\bar{x}$．由于

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0 \quad (p(x))$$

所以在 K' 里

$$\bar{x}^n + \overline{a_{n-1}}\,\bar{x}^{n-1} + \cdots + \bar{a}_0 = \bar{0}$$

因此，假如我们把 $\bar{x}$ 在 K 里的逆象叫做 α，我们就有

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

这样，域 K 包含一个 F 上的代数元 α．我们证明，$p(x)$ 就是 α 在 F 上的极小多项式．令 $p_1(x)$ 是 α 在 F 上的极小多项式．那么 $F[x]$ 中一切满足条件 $f(\alpha)=0$ 的多项式 $f(x)$ 显然作成一个理想，而这个理想就是主理想 $(p_1(x))$（参看 Ⅳ，4，定理 1 的证明）．因此 $p(x)$ 能被 $p_1(x)$ 整除．但 $p(x)$ 不可约，所以一定有

$$p(x) = ap_1(x), \quad a \in F$$

但 $p(x)$ 和 $p_1(x)$ 的最高系数都是 1，所以 $a=1$，而

$$p(x) = p_1(x)$$

因此我们可以在域 K 中作单扩域 $F(\alpha)$，而 $F(\alpha)$ 能满足定理的要求．

实际上，$F(\alpha)=K$．这一点我们留给读者去证明．证完．

给了域 F 和 $F[x]$ 的一个最高系数为 1 的不可约多项式 $p(x)$，可能存在若干个单代数扩域，都满足定理 3 的要求．但我们有

定理 4 令 $F(\alpha)$ 和 $F(\beta)$ 是域 F 的两个单代数扩域，并且 α 和 β 在 F 上有相同的极小多项式 $p(x)$．那么 $F(\alpha)$ 和 $F(\beta)$ 同构．

证明 假定 $p(x)$ 的次数是 n．那么 $F(\alpha)$ 的元都可以写成 $\sum_{i=0}^{n-1} a_i\alpha^i$ 的形式，而 $F(\beta)$ 的元都可以写成 $\sum_{i=0}^{n-1} a_i\beta^i$ 的形式，这里 $a_i \in F$．映射

$$\sum_{i=0}^{n-1} a_i \alpha^i \longrightarrow \sum_{i=0}^{n-1} a_i \beta^i$$

显然是 $F(\alpha)$ 与 $F(\beta)$ 间的同构映射. 证完.

总起来，我们有

定理 5 在同构的意义下，存在而且仅存在域 F 的一个单扩域 $F(\alpha)$，其中 α 的极小多项式是 $F[x]$ 的给定的，最高系数为 1 的不可约多项式.

习 题

1. 令 E 是域 F 的一个扩域，而 $a \in F$. 证明，α 是 F 上的一个代数元，并且 $F(\alpha)=F$.

2. 令 F 是有理数域. 复数 i 和 $\frac{2i+1}{i-1}$ 在 F 上的极小多项式各是什么? $F(i)$ 与 $F\left(\frac{2i+1}{i-1}\right)$ 是否同构?

3. 详细证明，定理 3 中 α 在域 F 上的极小多项式是 $p(x)$.

4. 证明，定理 3 中的 $F(\alpha)=K$.

§3. 代 数 扩 域

上一节的结果告诉我们，把域 F 上一个超越元或一个代数元添加于 F 所得到的单扩域的结构完全不同.

我们有以下事实：设 E 是 F 的一个扩域，并且 E 含有 F 上的超越元. 那么总存在 E 的一个子域 T，

$$F \subset T \subset E$$

使得 T 是由添加 F 上的超越元于 F 而得到的，而 E 只含 T 上的代数元.

这一事实的证明已超出本书的范围. 这个事实告诉我们，一个扩域可以分成两部分：一个超越的、一个代数的部分. 我们以下

将不再讨论超越的扩域，而只对代数的扩域作一些进一步的研究.

定义 若域F的一个扩域E的每一个元都是F上的一个代数元，那么E叫做F的一个**代数扩域**(扩张).

我们首先提出以下问题：假定$E=F(S)$是添加集合S于域F所得的扩域，并且S的元都是F上的代数元，那么E的元是否都是F上的代数元？

为了解答这个问题，我们需要扩域的次数这一个概念.

假定E是域F的一个扩域. 那么对于E的加法和$F\times E$到E的乘法来说，E作成F上的一个向量空间. 作为F上的向量空间，E或者有一个维数n，n是正整数；或者是一个无限维空间.

定义 若是域F的一个扩域E作为F上的向量空间有维数n，那么n叫做**扩域E在F上的次数**，记做$(E:F)$. 这时E叫做域F的一个**有限扩域**；否则E叫做域F的一个**无限扩域**.

关于扩域的次数我们有重要的

定理1 令I是域F的有限扩域，而E是I的有限扩域.那么E也是F的有限扩域，并且

$$(E:F)=(E:I)(I:F)$$

证明 设$(I:F)=r$，$(E:I)=s$，而$\alpha_1,\alpha_2,\cdots,\alpha_r$是向量空间$I$在域$F$上的一个基，$\beta_1,\beta_2,\cdots,\beta_s$是向量空间$E$在域$I$上的一个基. 看$E$的元

$$\alpha_i\beta_j \quad (i=1,2,\cdots,r;\ j=1,2,\cdots,s)$$

我们只须证明，这rs个元是向量空间E在域F上的一个基. 设

$$\sum_{i,j}a_{ij}\alpha_i\beta_j=0 \qquad (a_{ij}\in F)$$

那么

$$\sum_j\Big(\sum_i a_{ij}\alpha_i\Big)\beta_j=0,\quad \sum_i a_{ij}\alpha_i\in I$$

由于β_j对于I来说线性无关，我们得

$$\sum_i a_{ij}\alpha_i = 0 \quad (j=1,2,\cdots,s)$$

但 α_i 对于 F 来说线性无关，因而

$$a_{ij}=0 \quad (i=1,2,\cdots,r;\ j=1,2,\cdots,s)$$

这就是说，以上的 rs 个 E 的元 $\alpha_i\beta_j$ 对于 F 来说线性无关．现在假定 ω 是 E 的一个任意元．因为 β_j 是 I 上的 E 的一个基，

$$\omega = \sum_j \theta_j\beta_j \quad (\theta_j\in I)$$

又由于 α_i 是 F 上的 I 的一个基，

$$\theta_j = \sum_i c_{ij}\alpha_i \quad (c_{ij}\in F)$$

这样，我们有

$$\omega = \sum_{i,j} c_{ij}\alpha_i\beta_j$$

这就证明了，$\alpha_i\beta_j$ 是向量空间 E 在域 F 上的一个基．证完．

定理 1 的一个直接结果是

推论 1 令 $F, F_1, \cdots, F_t$ 是域，其中后一个是前一个的有限扩域．那么以下等式成立：

$$(F_t:F)=(F_t:F_{t-1})(F_{t-1}:F_{t-2})\cdots(F_1:F)$$

现在我们证明下述几个定理来解答前面提出的问题．

定理 2 令 $E=F(\alpha)$ 是域 F 的一个单代数扩域．那么 E 是 F 的一个代数扩域．

证明 令 α 在 F 上的极小多项式的次数是 n．由 V，2，定理2，$E=F(\alpha)$ 的每一个元都可以唯一地表成

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} \quad (a_i\in F)$$

的形式．这就是说，元 $1,\alpha,\cdots,\alpha^{n-1}$ 作成 F 上向量空间 E 的一个基，因此 E 是 F 的一个 n 次有限扩域．令 β 是 E 的一个任意元．那么 $1,\beta,\beta^2,\cdots,\beta^n$ 这 $n+1$ 个元对于 F 来说线性相关，因此，在 F 中存在不都等于零的 $n+1$ 个元 $b_0,b_1,\cdots,b_n$，能使

$$b_0+b_1\beta+\cdots+b_n\beta^n=0$$

这就是说，E 的任意元都是 F 上的代数元，而 E 是 F 的代数扩域．证完．

由定理 2 的证明可以得到以下两个重要事实．

推论 2 令 $F(\alpha)$ 是域 F 的一个单代数扩域，而 α 在 F 上的极小多项式的次数是 n．那么 $F(\alpha)$ 是 F 的一个 n 次扩域．

推论 3 域 F 的有限扩域一定是 F 的代数扩域．

定理 3 令 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_t)$，其中每一个 α_i 都是域 F 上的代数元．那么 E 是 F 的有限扩域，因而是 F 的代数扩域．

证明 我们用归纳法．

由定理 2，当 $t=1$ 的时候，定理成立．

假定，当我们只添加 $t-1$ 个元 $\alpha_1,\alpha_2,\cdots,\alpha_{t-1}$ 于 F 时，定理成立，也就是说，假定 $F(\alpha_1,\alpha_2,\cdots,\alpha_{t-1})$ 是 F 的有限扩域．

现在来看 $F(\alpha_1,\alpha_2,\cdots,\alpha_t)$ 的情形．我们知道，

$$F(\alpha_1,\alpha_2,\cdots,\alpha_t)=F(\alpha_1,\alpha_2,\cdots,\alpha_{t-1})(\alpha_t)$$

由于 α_t 是 F 上的代数元，所以它也是 $F(\alpha_1,\cdots,\alpha_{t-1})$ 上的代数元．因此 $F(\alpha_1,\cdots,\alpha_t)$ 是 $F(\alpha_1,\cdots,\alpha_{t-1})$ 的单代数扩域，而由推论 2，$F(\alpha_1,\cdots,\alpha_t)$ 是 $F(\alpha_1,\cdots,\alpha_{t-1})$ 的有限扩域．

由于

$$F\subset F(\alpha_1,\alpha_2,\cdots,\alpha_{t-1})\subset F(\alpha_1,\alpha_2,\cdots,\alpha_t)$$

根据定理 1，$F(\alpha_1,\alpha_2,\cdots,\alpha_t)$ 是 F 的有限扩域，于是由推论 3，它是 F 的代数扩域．证完．

推论 4 一个域 F 上的两个代数元的和、差、积与商（分母不为零）仍是 F 上的代数元．

定理 4 令 $E=F(S)$，这里集合 S 只含域 F 上的代数元．那么 E 是 F 的代数扩域．

证明 令 β 是 E 的任意元．根据 V, 1, (1) 式，

$$\beta=\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)}$$

这里 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 S 中有限个元素，而 f_1 和 $f_2(\neq 0)$是 F 上这些 α 的多项式．这样 $\beta\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)$．于是由定理3，$\beta$ 是 F 上的代数元．证完．

习　题

1．令 E 是域 F 的一个代数扩域，而 α 是 E 上的一个代数元．证明，α 是 F 上的一个代数元．

2．令 F, I 和 E 是三个域，并且 $F\subset I\subset E$．假定

$$(I:F)=m$$

而 E 的元 α 在 F 上的次数是 n，并且$(m, n)=1$．证明，α 在 I 上的次数也是 n．

3．令域 F 的特征不是 2，E 是 F 的扩域，并且

$$(E:F)=4$$

证明：存在一个满足条件 $F\subset I\subset E$ 的 F 的二次扩域 I 的充分与必要条件是：$E=F(\alpha)$，而 α 在 F 上的极小多项式是

$$x^4+ax^2+b$$

4．令 E 是域 F 的一个有限扩域．那么总存在 E 的有限个元 α_1，α_2，$\cdots$，α_m，使

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_m)$$

5．令 F 是有理数域．看添加复数于 F 所得扩域：

$$E_1=F(2^{\frac{1}{3}},2^{\frac{1}{3}}i)$$

$$E_2=F(2^{\frac{1}{3}},2^{\frac{1}{3}}\omega i),\ \omega=\frac{-1+\sqrt{3}i}{2},\ \omega^3=1$$

证明：

$$(E_1:F(2^{\frac{1}{3}}))=2,\ (E_1:F)=6$$

$$(E_2:F(2^{\frac{1}{3}}))=4,\ (E_2:F)=12$$

§4. 多项式的分裂域

我们都知道，所谓代数基本定理是什么．这个定理告诉我们，复数域C上一元多项式环$C[x]$的每一个n次多项式在C里有n个根，换一句话说，$C[x]$的每一个多项式在$C[x]$里都能分解为一次因子的乘积．

若是一个域E上的一元多项式环$E[x]$的每一个多项式在$E[x]$里都能分解为一次因子的乘积，那么E显然不再有真正的代数扩域．这样的一个域叫做**代数闭域**．

我们有以下事实：对于每一个域F都存在F的代数扩域E，而E是代数闭域．

这一事实的证明也已超出本书的范围．但分裂域的理论可以在一定意义下弥补这一个缺陷．

定义 域F的一个扩域E叫做$F[x]$的n次**多项式$f(x)$在F上的一个分裂域(或根域)**，假如

(i) 在$E[x]$里(有时简称在E里)$f(x)$可以分解为一次因子的积：

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\quad(\alpha_i\in E)$$

(ii) 在一个小于E的中间域$I(F\subset I\subset E)$里，$f(x)$不能这样地分解．

按这个定义，E是一个使得$f(x)$能够分解为一次因子的F的最小扩域．我们先看一看，一个多项式的分裂域应该有什么性质．

定理1 令E是域F上多项式$f(x)$的一个分裂域：

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\quad(\alpha_i\in E)\tag{1}$$

那么$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$．

证明 我们有

$$F \subset F(\alpha_1, \alpha_2, \cdots, \alpha_n) \subset E$$

并且在 $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 中，$f(x)$已经能够分解成(1)的形式．因此根据多项式的分裂域的定义，

$$E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$$ 证完

根据这个定理，如果有 F 上的多项式 $f(x)$ 的分裂域 E 存在，那么 E 刚好是把 $f(x)$ 的根添加于 F 所得的扩域．因此我们也把多项式的分裂域叫做它的根域．现在我们证明多项式的分裂域的存在．

定理 2 给了域 F 上一元多项式环 $F[x]$ 的一个 n 次多项式 $f(x)$，一定存在 $f(x)$ 在 F 上的分裂域 E．

证明 假定在 $F[x]$ 里，

$$f(x) = f_1(x) g_1(x)$$

这里 $f_1(x)$是最高系数为 1 的不可约多项式．那么存在一个域

$$E_1 = F(\alpha_1)$$

而 α_1 在 F 上的极小多项式是 $f_1(x)$．

在 E_1 里 $f(\alpha_1)=0$，所以 $x-\alpha_1 \mid f(x)$．因此在 E_1 里

$$f(x) = (x-\alpha_1) f_2(x) g_2(x)$$

这里 $f_2(x)$是 $E_1[x]$里最高系数为 1 的不可约多项式．这样，存在一个域

$$E_2 = E_1(\alpha_2) = F(\alpha_1)(\alpha_2) = F(\alpha_1, \alpha_2)$$

而 α_2 在 E_1 上的极小多项式是 $f_2(x)$．

在 $E_2[x]$ 里

$$f(x) = (x-\alpha_1)(x-\alpha_2) f_3(x) g_3(x)$$

$f_3(x)$是 $E_2[x]$的最高系数为 1 的不可约多项式．这样我们又可以利用 $f_3(x)$来得到域 $E_3 = F(\alpha_1, \alpha_2, \alpha_3)$，使得在 $E_3[x]$ 里

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) f_4(x) g_4(x)$$

这样一步一步地我们可以得到域

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

使得在 $E[x]$ 里

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$ 证完

域 F 上一个多项式 $f(x)$ 当然可能有不同的在 F 上的分裂域。但是这些分裂域都同构. 要证明这一点，我们需要两个引理.

引理1 令 L 和 $\bar{L}$ 是两个同构的域. 那么多项式环 $L[x]$ 和 $\bar{L}[x]$ 也同构.

证明 令 $a\longleftrightarrow\bar{a}$ 是 L 与 $\bar{L}$ 间的同构映射. 我们规定一个 $L[x]$ 到 $\bar{L}[x]$ 的映射

$$\phi:\qquad \sum a_ix^i\longrightarrow\sum\bar{a}_ix^i$$

ϕ 显然是 $L[x]$ 与 $\bar{L}[x]$ 间的一一映射. 我们看 $L[x]$ 的两个元 $f(x)$ 和 $g(x)$:

$$f(x)=\sum a_ix^i\longrightarrow\sum\bar{a}_ix^i=\bar{f}(x)$$

$$g(x)=\sum b_ix^i\longrightarrow\sum\bar{b}_ix^i=\bar{g}(x)$$

那么

$$\sum(a_i+b_i)x^i\longrightarrow\sum(\overline{a_i+b_i})x^i=\sum(\bar{a}_i+\bar{b}_i)x^i$$

$$f(x)+g(x)\longrightarrow\bar{f}(x)+\bar{g}(x)$$

$$\sum_k\Big(\sum_{i+j=k}a_ib_j\Big)x^k\longrightarrow\sum_k\Big(\sum_{i+j=k}\overline{a_ib_j}\Big)x^k=\sum_k\Big(\sum_{i+j=k}\bar{a}_i\bar{b}_j\Big)x^k$$

$$f(x)g(x)\longrightarrow\bar{f}(x)\bar{g}(x)$$

所以 ϕ 是同构映射. 证完.

在上述同构映射 ϕ 之下，$L[x]$ 的一个不可约多项式的象显然是 $\bar{L}[x]$ 的一个不可约多项式.

引理2 令 L 与 $\bar{L}$ 是同构的域，$p(x)$ 是 $L[x]$ 的一个最高系数为1的不可约多项式，$\bar{p}(x)$ 是与 $p(x)$ 对应的 $\bar{L}[x]$ 的不可约多项式. 又假定 $L(\alpha)$ 与 $\bar{L}(\bar{\alpha})$ 各是 L 与 $\bar{L}$ 的单扩域，满足条件 $p(\alpha)=0$ 和 $\bar{p}(\bar{\alpha})=0$. 那么存在 $L(\alpha)$ 与 $\bar{L}(\bar{\alpha})$ 间的一个同构映射，并且这

个同构映射能够保持原来的 L 与 $\bar{L}$ 间的同构映射.

证明　假定 $p(x)$ 的次数是 n, 那么 $\bar{p}(x)$ 的次数也是 n. 这样,若 $a\longleftrightarrow\bar{a}$ 是 L 与 $\bar{L}$ 间的同构映射,那么

$$\phi:\qquad \sum_{i=0}^{n-1}a_i\alpha^i\longrightarrow\sum_{i=0}^{n-1}\bar{a}_i\bar{\alpha}^i$$

是一个 $L(\alpha)$ 与 $\bar{L}(\bar{\alpha})$ 间的一一映射. 看 $L(\alpha)$ 的两个元

$$f(\alpha)=\sum_{i=0}^{n-1}a_i\alpha^i,\quad g(\alpha)=\sum_{i=0}^{n-1}b_i\alpha^i$$

由于

$$\sum_{i=0}^{n-1}(a_i+b_i)\alpha^i\longrightarrow\sum_{i=0}^{n-1}(\overline{a_i+b_i})\bar{\alpha}^i=\sum_{i=0}^{n-1}(\bar{a}_i+\bar{b}_i)\bar{\alpha}^i$$

有
$$f(\alpha)+g(\alpha)\longrightarrow\bar{f}(\bar{\alpha})+\bar{g}(\bar{\alpha})$$

我们知道,$f(\alpha)g(\alpha)=r(\alpha)$,这里

$$f(x)g(x)=q(x)p(x)+r(x)$$

由引理 1 得

$$\bar{f}(x)\bar{g}(x)=\bar{q}(x)\bar{p}(x)+\bar{r}(x)$$
$$\bar{f}(\bar{\alpha})\bar{g}(\bar{\alpha})=\bar{r}(\bar{\alpha})$$

因此
$$f(\alpha)g(\alpha)=r(\alpha)\longrightarrow\bar{r}(\bar{\alpha})=\bar{f}(\bar{\alpha})\bar{g}(\bar{\alpha})$$

这样,ϕ 是 $L(\alpha)$ 与 $\bar{L}(\bar{\alpha})$ 间的同构映射.

至于 ϕ 能够保持原来 L 与 $\bar{L}$ 间的同构映射,显然. 证完.

现在我们证明一个多项式的分裂域的唯一性.

我们证明更一般的下述

定理 3　令 F 与 $\bar{F}$ 是同构的域,$F[x]$ 的 $f(x)$ 与 $\bar{F}[x]$ 的 $\bar{f}(x)$ 是在引理 1 的意义下相对应的 n 次多项式. 又假定

$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 $f(x)$ 在 F 上的一个分裂域,

$\bar{E}=\bar{F}(\beta_1,\beta_2,\cdots,\beta_n)$ 是 $\bar{f}(x)$ 在 $\bar{F}$ 上的一个分裂域,

那么在E与$\bar{E}$间存在一个同构映射ϕ，ϕ能够保持F与$\bar{F}$间的同构映射，并且可以分别掉换α_i和β_j的次序，使在ϕ之下，

$$\alpha_i \longleftrightarrow \beta_i$$

证明 我们已经知道：$F \cong \bar{F}$．假定对于$k<n$，我们能够分别掉换α_i和β_j的次序，使得

$$L = F(\alpha_1, \alpha_2, \cdots, \alpha_k) \cong \bar{F}(\beta_1, \beta_2, \cdots, \beta_k) = \bar{L}$$

这个同构映射保持F与$\bar{F}$间的同构映射，并且在这个同构映射之下，

$$\alpha_i \longleftrightarrow \beta_i \quad (i=1, 2, \cdots, k)$$

设在$L[x]$里

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)p_k(x)g_k(x)$$

这里$p_k(x)$是$L[x]$的一个最高系数为1的不可约多项式．由引理1，在$\bar{L}[x]$里

$$\bar{f}(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_k)\bar{p}_k(x)\bar{g}_k(x)$$

而$\bar{p}_k(x)$是$\bar{L}[x]$的一个最高系数为1的不可约多项式．

在$F(\alpha_1, \alpha_2, \cdots, \alpha_n)$和$\bar{F}(\beta_1, \beta_2, \cdots, \beta_n)$里，因子

$$p_k(x)g_k(x) \text{ 和 } \bar{p}_k(x)\bar{g}_k(x)$$

进一步分别分解为$(x-\alpha_{k+1})\cdots(x-\alpha_n)$和$(x-\beta_{k+1})\cdots(x-\beta_n)$．分别掉换$\alpha_{k+1}, \cdots, \alpha_n$和$\beta_{k+1}, \cdots, \beta_n$的次序，不妨假定

$$p_k(\alpha_{k+1}) = 0, \quad \bar{p}_k(\beta_{k+1}) = 0$$

于是由引理2，

$$L(\alpha_{k+1}) = F(\alpha_1, \alpha_2, \cdots, \alpha_{k+1}) \cong \bar{F}(\beta_1, \beta_2, \cdots, \beta_{k+1}) = \bar{L}(\beta_{k+1})$$

这个同构映射保持F与$\bar{F}$间的同构映射，并且在这个同构映射下

$$\alpha_i \longleftrightarrow \beta_i \quad (i=1, 2, \cdots, k+1)$$

证完

我们知道，一个n次多项式在一个域里最多有n个根(IV, 6, 推论1)．分裂域的存在定理告诉我们，域F上多项式$f(x)$在F的某一个扩域里一定有n个根．分裂域的唯一存在定理告诉我们，

用不同方法找到的 $f(x)$ 的两组根，抽象地来看，没有什么区别. 这样，给了任何一个域 F 和 F 上一个 n 次多项式 $f(x)$，我们总可以谈论 $f(x)$ 的 n 个根. 因此，分裂域的理论在一定意义下可以代替所谓代数基本定理.

在域 F 上一个多项式 $f(x)$ 的分裂域里，并不是只有 $f(x)$ 可以分解成一次因子的乘积. 我们有以下重要的

定理 4 令 E 是多项式 $f(x)$ 在域 F 上的分裂域，而 β 是 E 的一个任意元. 那么 β 在 F 上的极小多项式在 E 里分解为一次因子的乘积.

证明 令 $f(x)$ 在域 F 上的分裂域是

$$E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

假定 β 在 F 上的极小多项式 $g(x)$ 不能在 $E[x]$ 里分解为一次因子的乘积. 那么在 $E[x]$ 里

$$g(x) = (x-\beta)p(x)g_1(x)$$

而 $p(x)$ 是 $E[x]$ 中最高系数为 1 的不可约多项式，且 $g(x)$ 的次数 m 大于 1. 作单扩域

$$E(\beta') = F(\alpha_1, \alpha_2, \cdots, \alpha_n, \beta')$$

使得 $p(\beta')=0$. 我们看一看 $F(\beta')$. 由于

$$g(\beta') = (\beta'-\beta)p(\beta')g_1(\beta') = 0$$

根据 V, 2, 定理 4, 有

$$F(\beta') \cong F(\beta)$$

因而由引理 1, 有

$$F(\beta')[x] \cong F(\beta)[x]$$

而且在这个同构映射之下

$$f(x) \longleftrightarrow f(x)$$

这样，由定理 3, $f(x)$ 在 $F(\beta')$ 上的分裂域与 $f(x)$ 在 $F(\beta)$ 上的分裂域同构. 但 $f(\beta', \alpha_1, \cdots, \alpha_n)$ 是 $f(x)$ 在 $F(\beta')$ 上的一个分裂域

而 $F(\beta,\alpha_1,\cdots,\alpha_n)$ 是 $f(x)$ 在 $F(\beta)$ 上的一个分裂域．因此

$$F(\beta',\alpha_1,\cdots,\alpha_n)\cong F(\beta,\alpha_1,\cdots,\alpha_n)$$

$$(F(\beta',\alpha_1,\cdots,\alpha_n):F)=(F(\beta,\alpha_1,\cdots,\alpha_n):F)$$

但是我们显然有

$$(F(\beta',\alpha_1,\cdots,\alpha_n):F)=(E(\beta'):E)(E:F)=m(E:F)$$

$$\text{而}(F(\beta,\alpha_1,\cdots,\alpha_n):F)=(E:F)$$

由于 $m>1$，这是一个矛盾．证完．

在下两节中我们要用到分裂域的理论来讨论两种特殊类型的域．

习　　题

1．证明，有理数域 F 上多项式 x^4+1 的分裂域是一个单扩域 $F(\alpha)$，其中 α 是 x^4+1 的一个根．

2．令 F 是有理数域，x^3-a 是 F 上一个不可约多项式，而 α 是 x^3-a 的一个根．证明，$F(\alpha)$ 不是 x^3-a 在 F 上的分裂域．

3．令 $p_1(x),p_2(x),\cdots,p_m(x)$ 是域 F 上 m 个最高系数为 1 的不可约多项式．证明，存在 F 的一个有限扩域 $F(\alpha_1,\alpha_2,\cdots,\alpha_m)$，其中 α_i 在 F 上的极小多项式是 $p_i(x)$．

4．令 P 是一个特征为素数 p 的域，$F=P(\alpha)$ 是 P 的一个单扩域，而 α 是 $P[x]$ 的多项式 $x^p-\alpha$ 的一个根．$P(\alpha)$ 是不是 $x^p-\alpha$ 在 P 上的分裂域？

§5．有 限 域

我们要讨论的第一种特殊类型的域是有限域．有限域在实验设计和编码理论中都有应用．

定义　一个只含有限个元素的域叫做一个**有限域**．

例如，特征是 p 的素域就是一个有限域．

先看一看，一个有限域应该有什么性质．

定理 1　**一个有限域 E 有 p^n 个元素，这里 p 是 E 的特征而 n**

是E在它的素域Δ上的次数.

证明 E的特征一定是一个素数p,不然的话,E所含的素域已经有无限多个元,而E不可能是一个有限域.

把E所含的素域记作Δ. 因为E只含有限个元,所以它一定是Δ的一个有限扩域而$(E:\Delta)=n$. 这样,E的每一个元可以唯一地写成

$$a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n$$

的形式,这里$a_i\in\Delta$,而$\alpha_1,\alpha_2,\cdots,\alpha_n$是向量空间$E$在$\Delta$上的一个基. 由于$\Delta$只有$p$个元,所以对于每一个$a_i$有$p$种选择法,因而$E$一共有$p^n$个元. 证完.

定理2 令有限域E的特征是素数p,E所含素域是Δ,而E有$q=p^n$个元. 那么E是多项式

$$x^q-x$$

在Δ上的分裂域. 任何两个这样的域都同构.

证明 E的不等于零的元对于乘法来说,作成一个群. 这个群的阶是$q-1$,单位元是1. 所以

$$\alpha^{q-1}=1,\quad \alpha\in E,\quad \alpha\neq 0$$

由于$0^q=0$,所以有

$$\alpha^q=\alpha,\quad \alpha\in E$$

因此,用$\alpha_1,\alpha_2,\cdots,\alpha_q$来表示$E$的元,在$E$里多项式

$$x^q-x=\prod_{i=1}^{q}(x-\alpha_i)$$

而且显然

$$E=\Delta(\alpha_1,\alpha_2,\cdots,\alpha_q)$$

这样,E是多项式x^q-x在Δ上的分裂域.

但特征为p的素域都同构,而多项式x^q-x在同构的域上的分裂域也同构,所以任何有p^n个元素的有限域都同构. 证完.

现在我们证明有限域的存在.

定理 3 令 Δ 是特征为 p 的素域，而 $q=p^n$ $(n\geqslant 1)$. 那么多项式 x^q-x 在 Δ 上的分裂域 E 是一个有 q 个元的有限域.

证明 $E=\Delta(\alpha_1,\alpha_2,\cdots,\alpha_n)$，这里 α_i 是 $f(x)=x^q-x$ 在域 E 里的根. 由于 E 的特征是 p, $f(x)$ 的导数

$$f'(x)=p^n x^{q-1}-1=-1$$

所以 $f(x)$ 与 $f'(x)$ 互素. 这样，由 Ⅳ, 6, 推论 2, $f(x)$ 的 q 个根都不相同.

我们断言, $f(x)$ 的这 q 个根作成 E 的一个子域 E_1. 这是因为，由 Ⅲ, 4,

$$(\alpha_i-\alpha_j)^{p^n}=\alpha_i^{p^n}-\alpha_j^{p^n}=\alpha_i-\alpha_j$$

$$\left(\frac{\alpha_i}{\alpha_j}\right)^{p^n}=\frac{\alpha_i^{p^n}}{\alpha_j^{p^n}}=\frac{\alpha_i}{\alpha_j}\quad(\alpha_j\neq 0)$$

这就是说, $\alpha_i-\alpha_j$ 和 $\frac{\alpha_i}{\alpha_j}(\alpha_j\neq 0)$ 仍是 $f(x)$ 的根而属于 E_1, 因而 E_1 是 E 的一个子域.

但 E_1 含 Δ, 也含一切 α_i, 所以 E_1 就是多项式 x^q-x 在 Δ 上的分裂域. 这样 $E=E_1$, 而 E 恰好有 q 个元. 证完.

以上证明了，给了素数 p 和正整数 n, 有而且(抽象地来看)只有一个恰好含 p^n 个元的有限域存在.

我们知道，单扩域是比较容易掌握的一种扩域. 现在我们要进一步证明，一个有限域一定是它所含素域的一个单扩域. 我们先证明

引理 令 G 是一个有限交换群，而 m 是 G 的元的阶中最大的一个. 那么 m 能被 G 的每一元的阶整除.

证明 容易看出：若 a 和 b 是 G 的两个元, a 的阶是 l_1, b 的阶是 l_2, 而 $(l_1,l_2)=1$, 那么 ab 的阶是 l_1l_2(参看Ⅱ, 9, 习题3).

假定G的元c的阶n不能整除m. 那么有素数p存在,使

$$m=p^i m_1, \quad (p,m_1)=1$$
$$n=p^j n_1, \quad j>i$$

令m是元d的阶. 于是

$$a=d^{p^i}\text{的阶是 } m_1$$
$$b=c^{n_1}\text{的阶是 } p^j$$

于是根据前面的结论,

$$ab\text{ 的阶是}p^j m_1>m$$

这与m是G的元的阶中最大的一个的假设矛盾. 证完.

定理 4 一个有限域E是它的素域Δ的一个单扩域.

证明 设E含有q个元. E的非零元对于E的乘法来说作成一个交换群G,它的阶是$q-1$. 令m是G的元的阶中最大的一个,那么由引理

$$\alpha_i^m=1, \quad \text{对于任意 } \alpha_i\in G$$

这就是说,多项式x^m-1至少有$q-1$个不同的根. 因此由Ⅳ,6,推论,

$$m\geqslant q-1$$

但由Ⅱ,9,定理3,

$$m\leqslant q-1$$

由以上两个式子得$m=q-1$. 这就是说,G有一个元α,它的阶是$q-1$,因而G是一个循环群: $G=(\alpha)$.

这样,E是添加α于Δ所得单扩域:

$$E=\Delta(\alpha)$$

证完

习　题

1. 令F是一个含p^n个元的有限域. 证明,对于n的每一个[illegible]

存在并且只存在F的一个有p^m个元的子域L.

2. 一个有限域一定有比它大的代数扩域.

3. 令F是一个有限域，Δ是它所含素域，且$F=\Delta(\alpha)$. α是否必须是F的非零元所作成的乘群的一个生成元？

4. 令Δ是特征为2的素域. 找出$\Delta[x]$的一切三次不可约多项式.

§6* 可离扩域

我们要讨论的第二种特殊类型的域是可离扩域. 我们的主要目的是要证明，有限可离扩域都是单扩域.

定义 令F是一个域，E是F的一个代数扩域而α是E的一个元. 如果α在F上的极小多项式没有重根，那么α叫做F上的一个**可离元**. 如果E的每一个元都是F上的可离元，那么E叫做F的一个**可离扩域**；否则E叫做F的一个不可离扩域.

为了对于可离扩域有一些初步的了解，我们先看一看，一个不可约多项式什么时候有重根.

引理1 令$f(x)$是$F[x]$的一个不可约多项式，这里F是一个域. 若F的特征是∞，那么$f(x)$没有重根；若F的特征是p，那么$f(x)$有重根的充分与必要条件是：$f(x)=g(x^p)$，这里$g(x)$是$F[x]$的一个多项式.

证明 $f(x)$有重根的充分与必要条件是：$f(x)$与它的导数$f'(x)$在$F[x]$中有次数$\geqslant 1$的公因子；由于$f(x)$不可约，这个条件只在$f'(x)=0$时才能被满足. 令

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

那么
$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$$

情形1. F的特征是∞. 这时

$$f'(x)=0\Longrightarrow a_n=a_{n-1}=\cdots=a_1=0$$

也就是说，$f(x)=a_0$，与$f(x)$不可约的假设矛盾. 所以在这个情形

下 $f(x)$ 不能有重根.

情形 2. F 的特征是 p. 这时

$$f'(x)=0 \Longrightarrow a_1=2a_2=\cdots=na_n=0$$

这就是说，只要 $i\neq 0\ (p)$，就必有 $a_i=0$. 因此

$$\begin{aligned} f(x) &= a_{tp}x^{tp}+\cdots+a_{2p}x^{2p}+a_px^p+a_0 \\ &= a_{tp}(x^p)^t+\cdots+a_{2p}(x^p)^2+a_px^p+a_0 \\ &= g(x^p) \end{aligned}$$

证完

由这个引理立刻得

定理 1 特征是∞的域的任何代数扩域都是可离扩域.

特征是 p 的域可以有不可离扩域.

引理 2 令 F 是一个特征为 p 的域. 当而且只当 F 的每一元 a 都是 F 的某一元 b 的 p 次幂：$a=b^p$ 时，F 的任何代数扩域都是可离扩域.

证明 假定 F 的每一元 a 都可以写成

$$a=b^p \quad (b\in F)$$

的形式. 这时 $F[x]$ 的一个多项式

$$f(x)=a_t(x^p)^t+a_{t-1}(x^p)^{t-1}+\cdots+a_1x^p+a_0$$

在 $F[x]$ 里一定可约. 因为令 $a_i=b_i^p$，就有

$$f(x)=(b_tx^t+b_{t-1}x^{t-1}+\cdots+b_1x+b_0)^p$$

这样，若 $F[x]$ 的一个多项式在 $F[x]$ 中不可约，那么它不能在 $F[x]$ 中写成 $g(x^p)$ 的形式. 于是根据引理 1，$F[x]$ 的每一不可约多项式都没有重根，因而 F 的代数扩域都是可离扩域.

现在反过来假定，F 含有元 a 而 $a\neq b^p (b\in F)$. 看 $F[x]$ 的多项式

$$f(x)=x^p-a$$

作 $f(x)$ 在 F 上的分裂域 E. 在 E 中 $f(x)$ 有 p 个根. 令其中的一个为 β，那么 $\beta^p=a$，因而由假设，β 不属于 F. 设 β 在 F 上的极小

多项式是 $k(x)$，那么 $k(x)\mid f(x)$. 但在 $E[x]$中

$$f(x)=x^p-\alpha=x^p-\beta^p=(x-\beta)^p$$

所以在$E[x]$中

$$k(x)=(x-\beta)^n$$

并且由于β不属于 F，这里的 $n>1$. 这样β在F上的极小多项式 $k(x)$有重根，因而E就是F的一个不可离扩域. 证完.

满足引理 2 的条件的域是存在的. 例如有限域.

定理 2 有限域的任何代数扩域都是可离扩域.

证明 令有限域F的特征是p，并且F含q个元：

$$a_1, a_2, \cdots, a_q$$

考察F的元

$$a_1^p, a_2^p, \cdots, a_q^p$$

由于当$i\neq j$时，

$$a_i^p-a_j^p=(a_i-a_j)^p\neq 0$$

所以 $a_1^p, a_2^p, \cdots, a_q^p$ 是 q 个不同的元，因而是F的全部元素. 因此F的每一元都是F的某个元的p次幂. 证完.

不满足引理 2 的条件的域F当然有不可离扩域，但这样的域F仍然可以有非平凡(即不属于 F)的可离元.

例 考虑特征是 3 的素域Δ的单超越扩域$F=\Delta(\xi)$. 元ξ显然不是F的某一个元的p次幂，因此F有不可离扩域. 但$F[x]$的多项式 $x^2-\xi$ 显然在F里不可约并且没有重根. 因此F有非平凡的可离元.

以下我们要证明，只要一个域F有非平凡的可离元，F就有真(即大于F的)可离扩域. 按照可离扩域的定义，这一点并不是显然的.

引理 3 令F是一个特征为p的域. 那么元α是F上的可离元的充分与必要条件是：$F(\alpha)=F(\alpha^p)$.

证明 假定α是F上的一个可离元. 这时，α一定是$F(\alpha^p)$

上的一个可离元．α 是 $F(\alpha^p)[x]$中多项式 $x^p-\alpha^p$ 的一个根．作这个多项式在 $F(\alpha^p)$上的分裂域 E，那么在 E 里

$$x^p-\alpha^p=(x-\alpha)^p$$

因此 α 在 $F(\alpha^p)$上的极小多项式可以在 E 里写成

$$(x-\alpha)^m \quad (1\leqslant m\leqslant p)$$

但 α 是 $F(\alpha^p)$上的可离元，所以 $m=1$．这样 α 在 $F(\alpha^p)$上的极小多项式是 $x-\alpha$．这就是说，$\alpha\in F(\alpha^p)$，从而

$$F(\alpha)=F(\alpha^p)$$

现在反过来假定，α 不是 F 上的可离元．这时，由引理 1，α 在 F 上的极小多项式是

$$f(x)=g(x^p)$$

由于 $f(x)$在 F 里不可约，所以 $g(x)$ 在 F 里也不可约．但 α^p 是多项式 $g(x)$ 的根，所以 α^p 在 F 上的极小多项式就是 $g(x)$．由于 $f(x)$ 和 $g(x)$ 的次数不同，所以 $F(\alpha)\neq F(\alpha^p)$．证完．

引理 4　令 E 是域 F 的单扩域：$E=F(\beta)$，而 β 是 F 上的一个可离元．若元 α 是 E 上的一个可离元，那么 α 也是 F 上的一个可离元．

证明　若 F 的特征是 ∞，引理成立．

假定 F 的特征是 p．

因为 α 是 $F(\beta)$上的可离元，所以由引理 3

$$F(\beta,\alpha)=F(\beta,\alpha^p)$$

令 β 在 $F(\alpha)$ 上的极小多项式是

$$g(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$$

$$b_i=\sum_j a_{ij}\alpha^j \quad (a_{ij}\in F)$$

那么，因为

$$b_i^p=\sum_j a_{ij}^p(\alpha^p)^j\in F(\alpha^p)$$

$$(g(x))^p = x^{np} + b_{n-1}^p x^{(n-1)p} + \cdots + b_1^p x^p + b_0^p$$

是 $F(\alpha^p)[x]$ 的一个多项式. 但 $(g(\beta))^p = 0$，所以 β 在 $F(\alpha^p)$ 上的极小多项式 $h(x)$ 整除 $(g(x))^p$. 因此有

$$g(x) | h(x) | (g(x))^p$$

但 β 是 F 上的一个可离元，因而也是 $F(\alpha^p)$ 上的一个可离元，所以必然有 $g(x) = h(x)$. 这就是说

$$(F(\alpha, \beta) : F(\alpha)) = (F(\alpha^p, \beta) : F(\alpha^p))$$

亦即 $$(F(\alpha, \beta) : F(\alpha)) = (F(\alpha, \beta) : F(\alpha^p))$$

于是，由于

$$F(\alpha^p) \subset F(\alpha) \subset F(\alpha, \beta)$$

我们有 $$F(\alpha) = F(\alpha^p)$$

这样，由引理 3，α 是 F 上的一个可离元. 证完.

应用引理 4，很容易得到

定理 3 若 α 与 β 是域 F 上的可离元. 那么 $F(\alpha, \beta)$ 是 F 的一个可离扩域.

证明 看 $F(\alpha, \beta)$ 的一个任意元 γ.

γ 是 $F(\alpha, \beta)$ 上的一个可离元，而 β 是 F 上的一个可离元，因而也是 $F(\alpha)$ 上的一个可离元，于是由引理 4，γ 是 $F(\alpha)$ 上的一个可离元. 由于 α 是 F 上的一个可离元，再一次应用引理 4，得 γ 是 F 上的一个可离元. 证完.

推论 若 α 和 β 是域 F 上的可离元，那么 $\alpha \pm \beta$，$\alpha\beta$ 和 $\frac{\alpha}{\beta}$（当 $\beta \neq 0$ 时）也是 F 上的可离元.

根据以上定理，给了一个域 F，除非 F 只有平凡的可离元，也就是说，除非 F 上的每一个次数大于 1 的、不是 $g(x^p)$ 形状的多项式都可约，F 就总有可离扩域. 这样，对最常遇到的特征为 ∞ 的域来说，根本没有不可离扩域. 而对特征为 p 的域来说，可离扩域出现的频率也要大得多. 所以可离扩域是较重要的一种扩域.

现在我们证明重要的

定理 4 域F的一个有限可离扩域E是F的单扩域.

证明 若F是一个有限域,那么E也是一个有限域. 这时,由于有限域是它所含素域Δ的单扩域,有

$$E=\Delta(\alpha)=F(\alpha)$$

而定理成立.

现在假定F有无限多个元素.

E既是F的一个有限扩域,就有

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

要证明这样的一个可离扩域是单扩域,显然只需证明:F的一个可离扩域$F(\beta,\gamma)$一定是F的单扩域.

令β在F上的极小多项式是$f(x)$,γ在F上的极小多项式是$g(x)$. 作多项式$f(x)g(x)$在$F(\beta,\gamma)$上的分裂域L. 那么在L里

$$f(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_s)$$

$$g(x)=(x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_t)$$

这里我们可以假定$\beta=\beta_1$, $\gamma=\gamma_1$.

我们看下列的一组方程:

$$(1)\qquad \beta_i+x\gamma_j=\beta_1+x\gamma_1\quad (i=1,2,\cdots,s;\ j=2,3,\cdots,t)$$

由于γ是F上的可离元,所以$g(x)$没有重根,而

$$\gamma_j\neq\gamma_1\quad (j=2,3,\cdots,t)$$

因此(1)中每一个方程在F里最多有一个解. 但F有无限多元,所以能在F中找出一个元$c\neq 0$来,使

$$\beta_i+c\gamma_j\neq\beta_1+c\gamma_1\quad (j\neq 1)$$

利用这个c,我们令

$$\theta=\beta_1+c\gamma_1=\beta+c\gamma$$

我们断言,$F(\beta,\gamma)=F(\theta)$. 令

$$h(x)=f(\theta-cx)$$

那么 $h(x)$ 和 $g(x)$ 都属于 $F(\theta)[x]$. 我们看一看在 $F(\theta)[x]$ 里这两个多项式的最大公因子是什么. 先考察，在 $L[x]$ 里它们的最大公因子是什么. 在 $L[x]$ 里

$$g(x)=(x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_t)$$

因此 $h(x)$ 和 $g(x)$ 在 $L[x]$ 里的最大公因子只能是若干 $(x-\gamma_j)$ 的乘积. 但由 c 的取法

$$\begin{aligned} h(\gamma_j)=f(\theta-c\gamma_j)=f(\beta_1+c\gamma_1-c\gamma_j)&\\ =f(\beta_1)=0, \text{若 } j=1&\\ \neq f(\beta_i)=0, \text{若 } j\neq 1& \end{aligned}$$

所以在 $L[x]$ 里，$h(x)$ 和 $g(x)$ 的最大公因子是 $x-\gamma$. 但求两个多项式的最大公因子，可以用辗转相除法，而在 $L[x]$ 里或 $F(\theta)[x]$ 里应用辗转相除法于 $h(x)$ 和 $g(x)$ 所得结果是一样的. 所以 $h(x)$ 和 $g(x)$ 在 $F(\theta)[x]$ 里的最大公因子也是 $x-\gamma$. 这就是说，$\gamma\in F(\theta)$，因而 $\beta=\theta-c\gamma\in F(\theta)$.

因此

$$F(\theta)=F(\beta,\gamma)$$

证完

习　题

1. 令域 F 的特征是 p. $f(x)$ 是 F 上一个不可约多项式，并且 $f(x)$ 可以写成 F 上 x^{p^e}，但不能写成 $x^{p^{e+1}}$ 的多项式($e\geqslant 1$). 证明，$f(x)$ 的每一个根的重复度都是 p^e.

2. 设域 F 没有不可离扩域. 证明，F 的任一代数扩域都没有不可离扩域.

3. 令域 F 的特征是 p 而 $E=F(\alpha,\beta)$，这里 α 是 F 上 n 次可离元而 β 是 F 上 p 次非可离元. $(E:F)=?$

4. 找一个域 F，使 F 有一个有限扩域 E 而 E 不是 F 的单扩域.

名词索引[①]

① 本索引以名词第一字笔划为序；第一字笔划相同时，以页数为序

七画

八画

九画

十画

十一画

十二画

十三画

十六画

十二画

十三画

十六画

第一章　基本概念

§1. 集　　合

1. $B\subset A$，但B不是A的真子集，这个情况什么时候才能出现？

解　由题设以及真子集的定义得，A的每一个元都属于B，因此$A\subset B$. 于是由

$$B\subset A \qquad A\subset B$$

得$A=B$. 所以上述情况在$A=B$时才能出现。

2. 假定$A\subset B$，$A\cap B=$？$A\cup B=$？

解　（i）　由于$A\subset B$，所以A的每一个元都属于B，即A的每一个元都是A和B的共同元，因而由交集的定义得

$$A\subset A\cap B$$

但显然有

$$A\cap B\subset A$$

所以

$$A\cap B=A$$

（ii）　由并集的定义，$A\cup B$的每一元素都属于A和B之一；但$A\subset B$，所以$A\cup B$的每一元素都属于B：

$$A\cup B\subset B$$

另一方面$B\subset A\cup B$，所以$A\cup B=B$。

§ 2. 映　射

1. $A=\{1, 2, \cdots, 100\}$. 找一个$A\times A$到A的映射。

解 用(a, b)表示$A\times A$的任意元素，这里a和b都属于A。按照定义做一个满足要求的映射即可，例如

$$\Phi:\quad (a, b)\longrightarrow a$$

就是这样的一个，因为Φ替$A\times A$的任何元素(a, b)规定了一个唯一的象a，而$a\in A$。

读者应该自己再找几个$A\times A$到A的映射。

2. 在你为习题1所找到的映射之下，是不是A的每一个元都是$A\times A$的一个元的象？

解 在上面给出的映射Φ之下，A的每一个元素都是$A\times A$的一个元的象，因为(a, b)中的a可以是A的任一元素。

你自己找到的映射的情况如何？有没有出现A的元素不都是象的情况？假如没有，找一个这样的映射。

§ 3. 代数运算

1. $A=\{$所有不等于零的偶数$\}$. 找一个集合D，使得普通除法是$A\times A$到D的代数运算。是不是找得到一个以上的这样的D？

解 一个不等于零的偶数除一个不等于零的偶数所得结果总是一个不等于零的有理数。

所以取

$$D=\{所有不等于零的有理数\}$$

普通除去就是一个 $A\times A$ 到D的代数运算。

可以找得到一个以上的满足要求的 D。读者可以自己找几个。

2. $A=\{a, b, c\}$。规定A的两个不同的代数运算。

解 （i）我们用运算表来给出 A的一个代数运算：o

	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

按照这个表，通过 o ，对于A的任何两个元素都可以得出一个唯一确定的结果 a 来，而 a 仍属于A。所以 o 是A的一个代数运算。

这个代数运算也可以用以下方式来加以描述

o： $(x, y)\longrightarrow a=x\text{o}y$ 对一切 $x, y\in A$

（ii） 同理

o： $(x, y)\longrightarrow x=x\text{o}y$ 对一切 $x, y\in A$

也是A的一个代数运算．读者可用列表的方法来给出这个代数运算。

读者还应自己给出几个A的代数运算。

§ 4. 结合律

1. $A=\{所有不等于零的实数\}$．o是普通除法：

$$a \circ b = \frac{a}{b}$$

这个代数运算适合不适合结合律?

解 这个代数运算 $\circ$ 不适合结合律. 例如,

当

$$a = 4 \qquad b = c = 2$$

时

$$(a \circ b) \circ c = (4 \circ 2) \circ 2 = \frac{4}{2} \circ 2 = \frac{2}{2} = 1$$

$$a \circ (b \circ c) = 4 \circ (2 \circ 2) = 4 \circ \left(\frac{2}{2}\right) = \frac{4}{1} = 4$$

所以当 a, b 和 c 取上述值时

$$(a \circ b) \circ c \neq a \circ (b \circ c)$$

2. $A = \{$所有实数$\}$. 代数运算

$\circ$: $(a, b) \longrightarrow a + 2b = a \circ b$

适合不适合结合律?

解 读者可以用解上一题的方法来证明, 所给代数运算不适合结合律.

3. $A = \{a, b, c\}$. 由表

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

给出的代数运算适合不适合结合律?

解 所给代数运算o适合结合律。为了得出这个结论，需要对元素a，b，c的27（$=3^3$）种排列（元素允许重复出现）加以验证。但是利用元素a的特性，可以把验证简化。仔细考察运算表，我们发现以下规律：对集合A的任意元素x来说，都有

$$a\circ x=x\circ a=x$$

由此得出，对于有a出现的排列，结合律都成立。这一点读者可以自己验证。还剩下a不出现的排列。这样的排列共有8（$=2^3$）种。我们在这里验证4种，其余4种读者可以自己验证。

$$(b\circ b)\circ b=c\circ b=a$$
$$b\circ(b\circ b)=b\circ c=a$$

所以 $$(b\circ b)\circ b=b\circ(b\circ b)$$

$$(b\circ b)\circ c=c\circ c=b$$
$$b\circ(b\circ c)=b\circ a=b$$

所以 $$(b\circ b)\circ c=b\circ(b\circ c)$$

$$(b\circ c)\circ b=a\circ b=b$$
$$b\circ(c\circ b)=b\circ a=b$$

所以 $$(b\circ c)\circ b=b\circ(c\circ b)$$

$$(b\circ c)\circ c=a\circ c=c$$
$$b\circ(c\circ c)=b\circ b=c$$

所以 $$(b\circ c)\circ c=b\circ(c\circ c)$$

§5. 交换律

1. $A=\{$所有实数$\}$，o是普通减法：

$$a \circ b = a - b$$

这个代数运算适合不适合交换律？

解 容易验证，当 $a=1$，$b=2$ 时

$$a \circ b \neq b \circ a$$

所以这个代数运算不适合交换律。

2. $A=\{a, b, c, d\}$。由表

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	d
d	d	c	a	b

所给的代数运算适合不适合交换律？

解 要回答这个问题，只须考察一下运算表，看一看关于主对角线对称的位置上，有没有不相同的元素。

§ 6. 分配律

假定$\odot$，$\oplus$是A的两个代数运算，并且$\oplus$适合结合律，$\odot$，$\oplus$适合两个分配律。证明

$$(a_1 \odot b_1) \oplus (a_1 \odot b_2) \oplus (a_2 \odot b_1) \oplus (a_2 \odot b_2)$$
$$= (a_1 \odot b_1) \oplus (a_2 \odot b_1) \oplus (a_1 \odot b_2) \oplus (a_2 \odot b_2)$$

解 $(a_1 \odot b_1) \oplus (a_1 \odot b_2) \oplus (a_2 \odot b_1) \oplus (a_2 \odot b_2)$

$$= a_1 \odot (b_1 \oplus b_2) + a_2 \odot (b_1 \oplus b_2)$$
$$= (a_1 \oplus a_2) \odot (b_1 \oplus b_2)$$
$$= (a_1 \oplus a_2) \odot b_1 \oplus (a_1 \oplus a_2) \odot b_2$$
$$= (a_1 \odot b_1) \oplus (a_2 \odot b_1) \oplus (a_1 \odot b_2) \oplus (a_2 \odot b_2)$$

§ 7. 一一映射、变换

1. A = { 所有 >0 的实数 }. $\overline{A}$ = { 所有实数 }. 找一个 A 与 $\overline{A}$ 间的一一映射.

解 Φ: $\quad x \longrightarrow \lg x \quad$ 对一切 $x \in A$

是一个 A 与 $\overline{A}$ 间的一一映射.

首先，给了任一 $x \in A$，即任一大于 0 的实数 x，$\lg x$ 是一个实数，即 $\lg x \in \overline{A}$，并且 $\lg x$ 是唯一确定的，所以 Φ 是一个 A 到 $\overline{A}$ 的映射.

其次，对于任一 $y \in \overline{A}$，即任一实数 y，$10^y = x$ 是一个大于 0 的实数，而在 Φ 之下，

$$x \longrightarrow \lg x = \lg 10^y = y$$

所以 Φ 是一个 A 到 $\overline{A}$ 的满射.

最后，若是 x_1，$x_2 \in A$，并且 $x_1 \neq x_1$，那么 $\lg x_1 \neq \lg x_2$，所以 Φ 是一个 A 到 $\overline{A}$ 的单射.

这样，Φ 是一个 A 与 $\overline{A}$ 间的一一映射.

2. A = { 所有 ≥ 0 的实数 }

$\overline{A}$ = { 所有实数 $\bar{a}$，$0 \leq \bar{a} \leq 1$ }

找一个 A 到 $\overline{A}$ 的满射.

解 Φ: $\quad x \longrightarrow x \quad$ 若 $0 \leq x < 1$

$$x \longrightarrow \frac{1}{x} \quad 若\ x \geq 1$$

是一个 A 到 $\overline{A}$ 的满射.

首先，Φ 替每一 $x \in A$ 规定了一个唯一确定的象 $\Phi(x)$，

而 $0\leq\Phi(x)\leq 1$，所以Φ是一个A到$\overline{A}$的映射。其次，在Φ之下，$\overline{A}$的每一元$\overline{a}$都是A中一个元，即$\overline{a}$本身的象，所以Φ是一个A到$\overline{A}$的满射。

读者可以证明：

Φ_1:　　$x\longrightarrow|\sin x|$　　$x\in A$

Φ_2:　　$x\longrightarrow 0$　　$0\leq x<1$

$x\longrightarrow\frac{1}{x}$　　$x\geq 1$

都是A到$\overline{A}$的满射。

3. 假定Φ是A与$\overline{A}$间的一个一一映射，a是A的一个元。

$$\Phi^{-1}[\Phi(a)]=?\qquad \Phi[\Phi^{-1}(a)]=?$$

若Φ是A的一个一一变换，这两个问题的回答又该是什么？

解　当Φ是A与$\overline{A}$间的一个一一映射时，

$\Phi^{-1}[\Phi(a)]=a$　　$\Phi[\Phi^{-1}(a)]$未必有意义。

若Φ是A的一个一一变换，那么

$$\Phi^{-1}[\Phi(a)]=a\qquad \Phi[\Phi^{-1}(a)=a$$

读者可以做一做以下补充习题。

(i)　$A=\{$所有≥ 0的整数$\}$

$\overline{A}=\{$所有>0的整数$\}$

证明

Φ:　　$x\longrightarrow x+1$　　对一切$x\in A$

是A与$\overline{A}$间的一个一一映射。

(ii)　$A=\{$所有≥ 0的实数$\}$

$$\overline{A} = \{所有>0的实数\}$$

利用（i）题找一个A与$\overline{A}$间的一一映射。

§8. 同　态

1. $A=\{所有实数x\}$。A的代数运算是普通乘法。以下映射是不是A到A的一个子集$\overline{A}$的同态满射？

$a)$ $x \to |x|$　　$b)$ $x \to 2x$　　$c)$ $x \to x^2$

$d)$ $x \to -x$

解　$a)$　取$\overline{A}=\{所有\geq 0的实数\}$，则$\overline{A} \subset A$，而

Φ_1:　　$x \to |x| = \Phi_1(x)$　　$x \in A$

是A到$\overline{A}$的一个同态满射。因为：对任一实数x，$|x|$是一个唯一确定的≥ 0的实数，所以Φ_1是A到$\overline{A}$的一个映射；若是$\bar{x} \in \overline{A}$，那么$\bar{x} \in A$，

而

$$\Phi_1(\bar{x}) = |\bar{x}| = \bar{x}$$

所以Φ_1是A到$\overline{A}$的一个满射；对任意x，$y \in A$，

$$\Phi_1(xy) = |xy| = |x||y| = \Phi_1(x)\Phi_1(y)$$

所以Φ_1是A到$\overline{A}$的一个同态满射。

$b)$　当x取遍一切实数值时，$2x$也取遍一切实数值。读者容易证明

Φ_2:　　$x \to 2x = \Phi_2(x)$

是A到A的一个满射，但Φ_2不是A到A的一个同态满射。因为：取A的数2和3，那么

$$\Phi_2(2) = 4 \qquad \Phi_2(3) = 6$$

$$\Phi_2\ (2.3)=\Phi_2(6)=12\neq\Phi_2(2)\ \Phi_2(3)$$

c）取$\overline{A}$＝｛所有≥ 0的实数｝，那么$\overline{A}\subset A$。读者可以自己证明

Φ_3：　　$x\to x^2=\Phi_3(x)$　　$x\in A$

是A到$\overline{A}$的一个同态满射。

d）　当x取遍一切实数值时，$-x$也取遍一切实数值。容易证明

Φ_4：　　$x\to -x=\Phi_4(x)$　　$x\in A$

是A到A的一个满射，但不是一个同态满射。

2． 假定A和$\overline{A}$对于代数运算$\circ$和$\bar{\circ}$来说同态，而$\overline{A}$和$\overline{\overline{A}}$对于代数运算$\bar{\circ}$和$\bar{\bar{\circ}}$来说同态。证明，A和$\overline{\overline{A}}$对于代数运算$\circ$和$\bar{\bar{\circ}}$说同态。

解　由题设存在A到$\overline{A}$的一个同态满射

Φ_1：　　$a\to\overline{a}=\Phi_1(a)$　　$a\in A$，$\overline{a}\in\overline{A}$

并且对于A的任意两个元素a和b来说

$$\Phi_1\ (a\circ b)\ =\overline{a}\ \bar{\circ}\ \overline{b}=\Phi_1(a)\ \bar{\circ}\ \Phi_1(b)$$

同样存在$\overline{A}$到$\overline{\overline{A}}$的一个同态满射

Φ_2：　　$\overline{a}\to\overline{\overline{a}}=\Phi_2\ (\overline{a})$　　$\overline{a}\in\overline{A}$，$\overline{\overline{a}}\in\overline{\overline{A}}$

并且对于$\overline{A}$的任意两个元素$\overline{a}$和$\overline{b}$来说

$$\Phi_2\ (\overline{a}\ \bar{\circ}\ \overline{b})\ =\overline{\overline{a}}\ \bar{\bar{\circ}}\ \overline{\overline{b}}=\Phi_2\ (\overline{a})\ \bar{\bar{\circ}}\ \Phi_2\ (\overline{b})$$

如下定义

Φ：　　$a\to\Phi_2[\Phi_1(a)]$　　$a\in A$

那么Φ是A到$\overline{\overline{A}}$的一个同态满射。因为：

（i）　由于Φ_1和Φ_2是同态满射，所以对于任何$a\in A$，$\Phi_1(a)$是$\overline{A}$的一个唯一确定的元素，而$\Phi_2[\Phi_1(a)]$是$\overline{\overline{A}}$的一个唯一确定的元素，因而Φ是A到$\overline{\overline{A}}$的一个映射。

(ii) 由于同一原因，对于任何$\overline{\overline{a}} \in \overline{\overline{A}}$，存在一个元素$\overline{a} \in \overline{A}$，使$\Phi_2(\overline{a}) = \overline{\overline{a}}$，并且存在一个元素$a \in A$，使$\Phi_1(a) = \overline{a}$，因此在$\Phi$之下，

$$a \to \Phi_2[\Phi_1(a)] = \Phi_2(\overline{a}) = \overline{\overline{a}}$$

而Φ是A到$\overline{\overline{A}}$的一个满射。

(iii) 由于同一原因，对于A的任何两个元素a和b

$$\begin{aligned}\Phi(a \circ b) &= \Phi_2[\Phi_1(a \circ b)] = \Phi_2[\Phi_1(a) \bar{\circ} \Phi_1(b)] \\ &= \Phi_2[\Phi_1(a)] \bar{\bar{\circ}} \Phi_2[\Phi_1(b)] \\ &= \Phi(a) \bar{\bar{\circ}} \Phi(b)\end{aligned}$$

而Φ是A到$\overline{\overline{A}}$的一个同态满射。

§ 9. 同构、自同构

1. $A = \{a, b, c\}$. 代数运算$\circ$由下表给定：

	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

找出所有A的一一变换，对于代数运算$\circ$来说，这些一一变换是否都是A的自同构？

解 A共有$6\ (=3!)$个一一变换，即

Φ_1:	$a \to a$	$b \to b$	$c \to c$
Φ_2:	$a \to a$	$b \to c$	$c \to b$
Φ_3:	$a \to b$	$b \to c$	$c \to a$

Φ_4:　　$a \to b$　　$b \to a$　　$c \to c$

Φ_5:　　$a \to c$　　$b \to b$　　$c \to a$

Φ_6:　　$a \to c$　　$b \to a$　　$c \to b$

对于代数运算o来说，Φ_1和Φ_4是A的自同构，其余4个都不是。这是因为，若Φ_i是一个A的自同构，那么对A的任何元素x和y，将有

(1)　　$\Phi_i(x \circ y) = \Phi_i(c) = \Phi_i(x) \circ \Phi_i(y) = c$

因而

(2)　　$\Phi_i(c) = c$

反过来，若（2）成立，那么（1）也成立。

2. $A = \{$所有有理数$\}$。找一个A的对于普通加法来说的自同构。（映射$x \to x$除外）。

解　设k是任一有理数，且$k \neq 0$，$k \neq 1$。

那么

Φ:　　$x \to kx$　　$x \in A$

是A的一个对于加法来说的自同构，并且Φ显然不是映射$x \to x$。Φ是A的一个一一变换，读者可以自己证明。令x和y是A的任意两个元素，那么

Φ:　$x + y \to \Phi(x+y) = k(x+y) = kx + ky = \Phi(x) + \Phi(y)$

所以Φ是A的一个自同构。

读者可以试证，A只有以下对于加法来说的自同构

$x \to kx$　　$x \in A$，k是$\neq 0$的有理数

3. $A = \{$所有有理数$\}$；A的代数运算是普通加法。$\overline{A} = \{$所有$\neq 0$的有理数$\}$；$\overline{A}$的代数运算是普通乘法。证明，对于给的代数运算来说，A与$\overline{A}$间没有同构映射存在。（先决定0在一个同构映射下的象。）

解 设Φ是A与$\overline{A}$间对于所给代数运算的一个同构映射，而$\Phi(0)=\overline{a}$。那么由于Φ是同构映射，有

$$\Phi(0)=\Phi(0+0)=\Phi(0)\Phi(0)=\overline{a}^2$$

但同构映射是单射，所以得$\overline{a}=\overline{a}^2$。于是有

$$\overline{a}^2-\overline{a}=\overline{a}(\overline{a}-1)=0$$

但$\overline{a}\in\overline{A}$，所以$\overline{a}\neq 0$，因而$\overline{a}-1=0$，即$\overline{a}=1$。这样

$$\Phi(0)=1 \qquad (1)$$

由于Φ是满射，$\overline{A}$的元-1必是A的某一元a的象：

$$\Phi(a)=-1$$

由是得

$$\Phi(2a)=\Phi(a+a)=\Phi(a)\Phi(a)=(-1)^2=1$$

于是由Φ是单射，得$2a=0$，即$a=0$，而$\Phi(0)=-1$，与（1）矛盾。这说明，在A与$\overline{A}$间对所给代数运算来说不存在同构对应。

读者可以用以下方法得出本题的另一证明：

设$\Phi(a)=2$。考虑$\Phi\left(\frac{a}{2}+\frac{a}{2}\right)$

§10. 等价关系与集合的分类

1. $A=\{$所有实数$\}$。A的元间的关系$>$以及$\geq$是不是等价关系？

解 $>$不是等价关系。这个关系不满足反射律：$a>a$不成立。

$\geq$也不是等价关系，它不满足对称律，例如，$3 \geq 2$，但$2 \geq 3$不成立。

2． 有人说：假如一个关系R适合对称律和推移律，那么它也适合反射律。他的推论方法是：因为R适合对称律

$$a\,R\,b \Longrightarrow b\,R\,a$$

因为R适合推移律

$$a\,R\,b,\quad b\,R\,a \Longrightarrow a\,R\,a$$

这个推论方法有什么错误？

解 这个推论方法的错误在于，对于“等价关系”定义的陈述没有准确地理解。

$$a\,R\,b \Longrightarrow b\,R\,a$$

的意思是：由$a\,R\,b$可得$b\,R\,a$；假如对于某一元素a，找不到任何元素b，使得$a\,R\,b$成立，那么就得不出$b\,R\,a$，因而也就得不出$a\,R\,a$。例如：令A是整数集，如下定义A的元间的关系R：

$$a\,R\,b \quad \text{当且仅当}\ ab > 0.$$

R显然满足对称律和推移律，但R不满足反射律，因为

$$0\,R\,0$$

不成立。

3． 仿照例3规定整数间的关系

$$a \equiv b \quad (-5)$$

证明你所规定的是一个等价关系，并且找出模－5的剩余类。

解 可以完全仿照例3来做。

第二章　群论

§1.　群的定义

1.　全体整数的集合对于普通减法来说是不是一个群？

解　不是，因为普通减法不适合结合律。

例如

$$3-(2-1)=3-1=2 \qquad (3-2)-1=1-1=0$$

$$3-(2-1)\neq(3-2)-1$$

2.　举一个有两个元的群的例。

解　令$G=\{e,\ a\}$，G的乘法由下表给出

	e	a
e	e	a
a	a	e

首先，容易验证，这个代数运算满足结合律

(1)　　$(xy)z=x(yz)$　　$x,\ y,\ z\in G$

因为，由于$ea=ae=a$，若是元素e在（1）中出现，那么（1）成立。（参考第一章，§4，习题3.）若是e不在（1）中出现，那么有

$$(aa)a=ea=a \qquad a(aa)=ae=a$$

而（1）仍成立。

其次，G有左单位元，就是e；e有左逆元，就是e，a有左逆元，就是a。所以G是一个群。

读者可以考虑一下，以上运算表是如何作出的。

3. 证明，我们也可以用条件Ⅰ，Ⅱ以及下面的条件Ⅳ′，Ⅴ′来做群的定义：

Ⅳ′ G里至少存在一个右逆元a^{-1}，能让

$$ae = a$$

对于G的任何元a都成立；

Ⅴ′ 对于G的每一个元a，在G里至少存在一个右逆元a^{-1}，能让

$$aa^{-1} = e$$

解 这个题的证法完全平行于本节中关于可以用条件Ⅰ，Ⅱ，Ⅳ，Ⅴ来做群定义的证明，但读者一定要自己写一下。

§2. 单位元、逆元、消去律

1. 若群G的每一个元都适合方程$x^2 = e$，那么G是交换群。

解 令a和b是G的任意两个元。由题设

$$(ab)(ab) = (ab)^2 = e$$

另一方面

$$(ab)(ba) = ab^2a = aea = a^2 = e$$

于是有 $(ab)(ab) = (ab)(ba)$。利用消去律，得

$$ab = ba$$

所以G是交换群。

2. 在一个有限群里，阶大于2的元的个数一定是偶数。

解 令G是一个有限群。设G有元a而a的阶$n>2$。考察a^{-1}。我们有

$$a^n(a^{-1})^n=e \qquad e(a^{-1})^n=(a^{-1})^n=e$$

设正整数$m<n$而$(a^{-1})^m=e$，那么同上可得$a^m=e$，与n是a的阶的假设矛盾。这样，n也是a^{-1}的阶，易见$a^{-1}\neq a$。否则

$$a^2=aa^{-1}=e$$

与$n>2$的假设矛盾。这样，我们就有一对不同的阶大于2的元a和a^{-1}。

设G还有元b，$b\neq a$，$b\neq a^{-1}$，并且b的阶大于2。那么b^{-1}的阶也大于2，并且$b^{-1}\neq b$。我们也有$b^{-1}\neq a$。否则

$$e=b^{-1}b=aa^{-1}=b^{-1}a^{-1}$$

消去b^{-1}得$b=a^{-1}$，与假设矛盾。同样可证$b^{-1}\neq a^{-1}$。这样，除a和a^{-1}外，又有一对不同的阶大于2的元b和b^{-1}。

由于G是有限群，而G的阶大于2的元总是成对出现，所以G里这种元的个数一定是偶数。

3. 假定G是一个阶是偶数的有限群。在G里阶等于2的元的个数一定是奇数。

解 由习题2知，G里阶大于2的元的个数是偶数。但G只有一个阶是1的元，就是单位元e。于是由于G的阶是偶数，得G里阶等于2的元的个数是奇数。

4. 一个有限群的每一个元的阶都有限。

解 令G是一个有限群而a是G的任一元素，那么

$$a,\ a^2,\ a^3,\ \cdots$$

不能都不相等。因此存在正整数 i，j，$i>j$，使 $a^i=a^j$。用 a^{-j} 乘两边，得

(1)　　　　$a^{i-j}=e$

这样，存在正整数 $i-j$，使（1）成立。因此也存在最小的正整数 m，使 $a^m=e$，这就是说，元 a 的阶是 m。

§4.　群的同态

假定在两个群 G 和 $\bar{G}$ 的一个同态映射之下，$a\to\bar{a}$。a 与 $\bar{a}$ 的阶是不是一定相同？

解　不一定。例如，令 G 是本章§1中例2所给出的群而 $\bar{G}$ 是该节中例1所给出的群。那么读者容易证明

Φ:　　　　$n\to g$　　n 是 G 的任意元

是 G 到 $\bar{G}$ 的一个同态映射。但 G 的每一个元 $n\neq 0$ 都是无限阶的，而 g 的阶是1。

§5.　变换群

1．假定 τ 是集合 A 的一个非一一变换。τ 会不会有一个左逆元 τ^{-1} 使得 $\tau^{-1}\tau=\varepsilon$？

解　可能有。例如令 $A=\{$所有正整数$\}$，则

τ:　　　　$1\to 1$，　$n\to n-1$　　$n>1$

显然是 A 的一个非一一变换。而 A 的变换

τ^{-1}:　　　　$n\to n+1$　　$n\in A$

就能使 $\tau^{-1}\tau=\varepsilon$。

2. 假定A是所有实数作成的集合。证明，所有A的可以写成

$$x \to ax+b \qquad a\text{和}b\text{是有理数，}a\neq 0$$

形式的变换作成一个变换群。这个群是不是一个交换群？

解 令G是由一切上述变换作成的集合。考察G的任何两个元素

τ： $x \to ax+b$ a和b是有理数，$a\neq 0$

λ： $x \to cx+d$ c和d是有理数，$c\neq 0$

那么

$\tau\lambda$： $$x \to x^{\tau\lambda} = (ax+b)^{\lambda} = c\ (ax+b)+d$$
$$= (ca)x + (cb+d)$$

这里ca和$cb+d$都是有理数，并且$ca\neq 0$。

所以$\tau\lambda$仍属于G。

结合律对一般变换都成立，所以对上述变换也成立。

单位变换

ε： $$x \to x$$

属于G。

容易验证，τ在G中有逆，即

τ^{-1}： $$x \to \frac{1}{a}x + \left(-\frac{b}{a}\right)$$

因此G作成一个变换群。

但G不是一个交换群。令

τ_1： $$x \to x+1$$

τ_2： $$x \to 2x$$

那么

$\tau_1\tau_2$： $$x \to (x^{\tau_1})^{\tau_2} = (x+1)^{\tau_2} = 2x+2$$

$\tau_2\tau_1$:　　　$x \to (x^{\tau_2})^{\tau_1} = (2x)^{\tau_1} = 2x+1$

$$\tau_1\tau_2 \neq \tau_2\tau_1$$

3. 假定S是一个集合A的所有变换作成的集合。我们暂时仍用符号

τ:　　　$a \longrightarrow a' = \tau(a)$

来说明一个变换τ。证明，我们可以用

$\tau_1\tau_2$:　　　$a \longrightarrow \tau_1[\tau_2(a)] = \tau_1\tau_2(a)$

来规定一个S的乘法，这个乘法也适合结合律并且对于这个乘法来说，ε还是S的单位元。

解　令τ_1和τ_2是S的任意两个元而a是A的任意一个元。那么$\tau_2(a)$和$\tau_1[\tau_2(a)]$都是A的唯一确定的元。因此如上规定的$\tau_1\tau_2$仍是S的一个唯一确定的元而我们得到了一个S的乘法。

令τ_3也是S的一个任意元，那么

$$[(\tau_1\tau_2)\tau_3](a) = \tau_1\tau_2[\tau_3(a)] = \tau_1\{\tau_2[\tau_3(a)]\}$$

$$[\tau_1(\tau_2\tau_3)](a) = \tau_1[\tau_2\tau_3(a)] = \tau_1\{\tau_2[\tau_3(a)]\}$$

所以$(\tau_1\tau_2)\tau_3 = \tau_1(\tau_2\tau_3)$而乘法适合结合律。

令τ是S的任意元。由于对一切$a \in A$，都有$\varepsilon(a) = a$，所以

$$\varepsilon\tau(a) = \varepsilon[\tau(a)] = \tau(a)$$

$$\tau\varepsilon(a) = \tau[\varepsilon(a)] = \tau(a)$$

即$\varepsilon\tau = \tau\varepsilon = \tau$而$\varepsilon$仍是$S$的单位元。

4. 证明，一个变换群的单位元一定是恒等变换。

解　设G是由某一集合A的变换组成的一个变换群，而ε是G的单位元。任取G的一个元τ和A的一个元a。由于

$\varepsilon\tau=\tau$，有

$$a^{\varepsilon\tau}=(a^{\varepsilon})^{\tau}=a^{\tau}$$

由于τ是A的一个一一变换，所以$a^{\varepsilon}=a$而ε是A的恒等变换。

5. 证明，实数域上一切有逆的$n\times n$矩阵对于矩阵乘法来说，作成一个群。

解 这个题的解法很容易，这里从略。

§6. 置换群

1. 找出所有S_3的不能和$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$交换的元。

解 S_3有6个元：

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

其中的

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^2$$

显然可以和$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$交换。通过计算，易见其它三个元不能和$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$交换。

2. 把S_3的所有元写成不相连的循环置换的乘积。

解 $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=(1)$，$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(2\ 3)$

$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(1\ 2)$，$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(1\ 3)$，$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\ 2\ 3)$

$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(1\ 3\ 2)$

3. 证明：

（i）两个不相连的循环置换可以交换；

（ii）$(i_1 i_2 \cdots i_k)^{-1} = (i_k i_{k-1} \cdots i_1)$。

解 （i）看S_n的两个不相连的循环置换σ和τ。我们考察乘积$\sigma\tau$使数字1，2，…，n如何变动。有三种情况。

（a） 数字i在σ中出现，并且σ把i变成j。这时由于σ和τ不相连，j不在τ中出现，因而τ使j不变，所以$\sigma\tau$仍把i变成j。

（b） 数字k在τ中出现，并且τ把k变成l。这时k不在σ中出现，因而σ使k不变，所以$\sigma\tau$仍把k变成l。

（c）数字m不在σ和τ中出现。这时$\sigma\tau$使m不动。

如上考察$\tau\sigma$使数字1，2，…，n如何变动，显然得到同样的结果。因此$\sigma\tau = \tau\sigma$。

（ii） 由于 $(i_1 i_2 \cdots i_k)(i_k i_{k-1} \cdots i_1) = (1)$，所以

$$(i_1 i_2 \cdots i_k)^{-1} = (i_k i_{k-1} \cdots i_1)$$

4. 证明一个k－循环置换的阶是k。

解 一个k－循环置换$\pi = (i_1 i_2 \cdots i_k)$的一次方，二次方，…，$k$次方分别把$i_1$变成$i_2$，$i_3$，…，$i_1$。同理$\pi^k$把$i_2$变成$i_2$，…，把$i_k$变成$i_k$。因此$\pi^k = (1)$。由上面的分析，若是$l < k$，那么$\pi^l \neq (1)$。这就证明了，$\pi$的阶是$k$。

5. 证明S_n的每一个元都可以写成

$$(1\ 2),\ (1\ 3),\ \cdots,\ (1\ n)$$

这$n-1$个2－循环置换中的若干个的乘积。

解 由于每一个置换都可以写成不相连的循环置换的乘积，所以只须证明，一个循环置换可以写成若干个$(1\ i)$形的置换的乘积。设π是一个k－循环置换。我们分两个情形

加以讨论。

(a) 1在π中出现，这时π可以写成

$$(1\, i_1 i_2 \cdots i_{k-1})$$

容易验算

$$(1\, i_1 i_2 \cdots i_{k-1}) = (1\, i_1)(1\, i_2)\cdots(1\, i_{k-1})$$

(b) 1不在π中出现，这时

$$\pi = (i_1 i_2 \cdots i_k) = (1\, i_1 i_2 \cdots i_k)(1\, i_1)$$
$$= (1\, i_1)(1\, i_2)\cdots(1\, i_k)(1\, i_1)$$

§7. 循环群

1. 证明，一个循环群一定是交换群。

解 设循环群$G=(a)$。那么G的任何两个元都可以写成a^m和a^n(m，n是整数）的形式。但

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$$

所以G是一个交换群。

2. 假定群的元a的阶是n。证明a^r的阶是$\frac{n}{d}$，这里$d=(r,\ n)$是r和n的最大公因子。

解 由于$d \mid r$，$r=ds$，所以

$$(a^r)^{\frac{n}{d}} = (a^{ds})^{\frac{n}{d}} = (a^n)^s = e$$

现在证明，$\frac{n}{d}$就是a^r的阶。设a^r的阶为k。那么$k \leq \frac{n}{d}$。令

$$\frac{n}{d} = kq + r_1 \qquad 0 \leq r_1 \leq k-1$$

得

$$e=(a^r)^{\frac{n}{d}}=(a^r)^{kq+r_1}=(a^r)^{kq}(a^r)^{r_1}=(a^r)^{r_1}$$

但 $r_1<k$ 而 k 是 a^r 的阶，所以 $r_1=0$ 而

$$\frac{n}{d}=kq$$

于是得 $k\left|\frac{n}{d}\right.$。（参看本节定理的第二种情形。）

为了证明 $k=\frac{n}{d}$，只须反过来证明 $\frac{n}{d}\left|k\right.$。由 $a^{rk}=e$ 而 n 是 a 的阶，同上有 $n\mid rk$，因而 $\frac{n}{d}\left|\frac{r}{d}k\right.$。但 d 是 n 和 r 的最大公因子，所以 $\frac{n}{d}$ 和 $\frac{r}{d}$ 互素而有 $\frac{n}{d}\left|k\right.$。

3. 假定 a 生成一个阶是 n 的循环群 G。证明：a^r 也生成 G，假如 $(r, n)=1$（这就是说 r 和 n 互素）。

解 由习题 2，a^r 的阶是 n。所以

$$a^r,\ (a^r)^2,\ \cdots,\ (a^r)^{n-1},\ (a^r)^n=e$$

互不相同。但 G 只有 n 个元，所以

$$G=\{a^r,\ (a^r)^2,\ \cdots,\ (a^r)^n\}$$

而 a^r 生成 G。

4. 假定 G 是循环群，并且 G 与 $\bar{G}$ 同态。证明 $\bar{G}$ 也是循环群。

解 由于 G 与 $\bar{G}$ 同态，$\bar{G}$ 也是一个群。设 $G=(a)$，而在 G 到 $\bar{G}$ 的同态满射 Φ 下，$a\longrightarrow\bar{a}$。看 $\bar{G}$ 的任意元 $\bar{g}$。那么在 Φ 下，有 $a^m\in G$，使 $a^m\longrightarrow\bar{g}$。但 $a^m\longrightarrow\bar{a}^m$。所以 $\bar{g}=\bar{a}^m$。

这样，$\bar{G}$的每一元都是$\bar{a}$的一个乘方而$\bar{G}=(\bar{a})$。

5. 假定G是无限阶的循环群，$\bar{G}$是任何循环群。证明G与$\bar{G}$同态。

解 令$G=(a)$，$\bar{G}=(\bar{a})$。定义

$$\Phi: \quad a^m \longrightarrow \bar{a}^m$$

我们证明，Φ是G到$\bar{G}$的一个同态满射。

（i） 由于G是无限阶的循环群，G的任何元都只能以一种方法写成a^m的形式，所以在Φ之下，G的每一个元有一个唯一确定的象，而Φ是G到$\bar{G}$的一个映射。

（ii） $\bar{G}$的每一个元都可以写成$\bar{a}^m$的形式，因此它在Φ之下是G的元a^m的象，而Φ是G到$\bar{G}$的一个满射。

(iii) $$a^m a^n = a^{m+n} \longrightarrow \bar{a}^{m+n} = \bar{a}^m \bar{a}^n$$

所以Φ是G到$\bar{G}$的一个同态满射。

§8. 子 群

1. 找出S_3的所有子群。

解 S_3显然有以下子群：

S_3本身；$((1))=\{(1)\}$；

$((1\ 2))=\{(1\ 2),(1)\}$；

$((1\ 3))=\{(1\ 3),(1)\}$；

$((2\ 3))=\{(2\ 3),(1)\}$；

$((1\ 2\ 3))=\{(1\ 2\ 3),(1\ 3\ 2),(1)\}$。

若S_3的一个子群H含有$(1\ 2)$，$(1\ 3)$这两个2－循环置换，那么H含有

$(1\ 2)(1\ 3)=(1\ 2\ 3),\ (1\ 2\ 3)(1\ 2)=(2\ 3)$

因而$H=S_3$。同理，若是S_3的一个子群含有两个2-循环置换$(2\ 1)$，$(2\ 3)$或$(3\ 1)$，$(3\ 2)$，这个子群也必然是S_3。

用完全类似的方法，读者可以算出，若是S_3的一个子群含有一个2-循环置换和一个3-循环置换，那么这个子群也必然是S_3。

因此上面给出的6个子群是S_3的所有子群。

2. 证明，群G的两个子群的交集也是G的子群。

解 设H_1和H_2是G的子群。

令e是G的单位元。那么e属于H_1和H_2，因而

$$e\in H_1\cap H_2$$

而$H_1\cap H_2$不空。

令$a,\ b\in H_1\cap H_2$。那么a，b属于H_1和H_2。但H_1和H_2是子群。所以ab^{-1}属于H_1和H_2，因而属于$H_1\cap H_2$。

这就证明了，$H_1\cap H_2$是G的子群。

3. 取S_3的子集$S=\{(1\ 2),\ (1\ 2\ 3)\}$。S生成的子群包含哪些元？一个群的两个不同的子集会不会生成相同的子群？

解 见习题1的解。

4. 证明，循环群的子群也是循环群。

解 设循环群$G=(a)$而H是G的一个子群。

若H只含单位元$e=a^0$，则$H=(e)$是循环群。若H不仅含单位元，那么因为H是子群，它一定含有元a^m，其中m是正整数。令i是最小的使得a^i属于H的正整数，我们证明，这时$H=(a^i)$。看H的任一元a^t。令

$$t = iq + r \qquad 0 \leq r < i$$

那么 $a^t = a^{iq}a^r$。由于 a^t 和a^{iq} 都属于H，有

$$a^r = a^{-iq}a^t \in H$$

于是由假设 $r = 0$，$a^t = (a^i)^q$ 而$H = (a^i)$。

5. 找出模12的剩余类加群的所有子群。

解 模12的剩余类加群G是一个阶为12的循环群。因此由题 4，G的子群都是循环群。容易看出：

([0]) = [0]

([1]) = ([5]) = ([7]) = ([11]) = G

([2]) = ([10]) = {[2], [4], [6], [8], [10], [0]}

([3]) = ([9]) = {[3], [6], [9], [0]}

([4]) = ([8]) = {[4], [8], [0]}

([6]) = {[6], [0]}

是G的所有子群。

6. 假定H是群G的一个非空子集并且H的每一个元的阶都有限。证明，H作成一个子群的充要条件是：

$$a, \ b \in H \Longrightarrow ab \in H$$

解 由本节定理 1，条件显然是必要的。

要证明条件也是充分的，由同一定理，只须证明：

$$a \in H \Longrightarrow a^{-1} \in H$$

设 $a \in H$。由于H的每一元的阶都有限，所以 a 的阶是某一正整数 n 而$a^{-1} = a^{n-1}$。于是由所给条件得 $a^{-1} \in H$。

§9. 子群的陪集

1. 证明，阶是素数的群一定是循环群。

解 设群G的阶为素数p。在G中取一元$a \neq e$，则a生成G的一个循环子群(a)。设(a)的阶为n，那么$n \neq 1$。但由定理2，$n \mid p$，所以$n = p$而$G = (a)$是一个循环群。

2. 证明，阶是p^m的群（p是素数，$m \geq 1$）一定包含一个阶是p的子群。

解 设群G的阶是p^m。在G中取一元$a \neq e$，那么由定理3，a的阶$n \mid p^m$。但$n \neq 1$，所以$n = p^t$，$t \geq 1$。若$t = 1$，那么a的阶为p，而(a)是一个阶为p的子群。若$t > 1$，可取$b = a^{p^{t-1}}$，那么b的阶为p而(b)是一个阶为p的子群。

3. 假定a和b是一个群G的两个元，并且$ab = ba$，又假定a的阶是m，b的阶是n，并且$(m, n) = 1$。证明：ab的阶是mn。

解 设ab的阶是k。由$ab = ba$，得

$$(ab)^{mn} = a^{mn}b^{mn} = e$$

因此$k \mid mn$。我们反过来证明，$mn \mid k$。由

$$e = (ab)^{kn} = a^{kn}b^{kn} = a^{kn}$$

以及a的阶为m，得$m \mid kn$。但$(m, n) = 1$，所以$m \mid k$。同理$n \mid k$。又由$(m, n) = 1$，得$mn \mid k$。

这样，ab的阶$k = mn$。

4. 假定$\sim$是一个群G的元间的一个等价关系，并且对于G的任意三个元a，x，x'来说

$$ax \sim ax' \Longrightarrow x \sim x'$$

证明，与G的单位元e等价的元所作成的集合是G的一个子群。

解 令H是与e等价的元所成的集合。

由于 $e\sim e$，所以H不空。

设 a，$b\in H$。那么 $a\sim e$，$b\sim e$。$b\sim e$可写成

$$a^{-1}ab\sim a^{-1}a$$

因此由题设，$ab\sim a\sim e$ 而 $ab\in H$。

$a\sim e$可写成 $ae\sim aa^{-1}$，因此由题设，$e\sim a^{-1}$而$a^{-1}\in H$。

这样，H作成G的一个子群。

5. 我们直接下右陪集 Ha 的定义如下：Ha 刚好包含G的可以写成

$$h\ a \qquad (h\in H)$$

形式的元。由这个定义推出以下事实：G的每一个元属于而且只属于一个右陪集。

解 取任意元 $a\in G$。由于 H 是一个子群，单位元 $e\in H$，因此 $a=e\ a\in H\ a$，这就是说，元 a 属于右陪集 $H\ a$。

设 $a\in H\ b$，$a\in H\ c$，那么

$$a=h_1b=H_2c \qquad (h_1,\ h_2\in H)$$

由此得，$b=h_1^{-1}h_2\ c$，而$H\ b$的任意元

$$hb=hh_1^{-1}h_2\ c\ \in H\ c$$

因而$H\ b\subset H\ c$。同样可证$H\ c\subset H\ b$。这样 $Hb=Hc$ 而 a 只能属于一个右陪集。

6. 若我们把同构的群看成一样的，一共只存在两个阶是 4 的群，它们都是交换群。

解 先给出两个阶是 4 的群。

模 4 的剩余类加群$G_1=\{[0],[1],[2],[3]\}$。G_1的元[1]的阶是 4 而G_1是[1]所生成的循环群([1])。

S_4的的子群

$$B_4=\{(1),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (14)(2\ 3)\}$$

叫作克莱因四元群. B_4是S_4的子群容易验证. 我们有

$$[(1\ 2)(3\ 4)]^2=[(1\ 3)(2\ 4)]^2=[(14)(23)]^2=(1)$$

$$(12)(34)(1\ 3)(24)=(13)(24)(12)(3\ 4)=(14)(23)$$

$$(13)(24)(14)(23)=(1\ 4)(2\ 3)(1\ 3)(2\ 4)=(12)(34)$$

$$(14)(23)(12)(34)=(1\ 2)(3\ 4)(1\ 4)(2\ 3)=(13)(24)$$

这两个群显然都是交换群。

现在证明，任何阶是 4 的群都和以上两个群之一同构。设G是一个阶为 4 的群。那么G的元的阶只能是 1，2 或 4.

若G有一个阶为 4 的元d，那么$G=(d)$是一个循环群而G与G_1同构。

若G没有阶为 4 的元，那么除单位元e外，G的其它 3 个元的阶都是 2．因此有

$$G=\{e,\ a,\ b,\ c\}\qquad a^2=b^2=c^2=e$$

由于G是群，有$ab\in G$。我们证明，$ab=c$。

由$ab=e$将得$ab=a^2$和$b=a$，这不可能。

由$ab=a$将得$b=e$，也不可能。

由$ab=b$将得$a=e$，也不可能。

因此只能$ab=c$．同样可证

$$ab=ba=c,\qquad bc=cb=a,\qquad ca=ac=b$$

比较G和B_4的代数运算，易见G和B_4同构。

补充题　利用 6 题证明，一个有限非交换群至少有 6 个元。

§10. 不变子群、商群

1. 假定群G的不变子群N的阶是2。证明，G的中心包含N。

解 令$N=\{e, n\}$，这里e是G的单位元。取G的任意元a。由于N是一个不变子群，有$aN=Na$，即

$$\{a, an\}=\{a, na\}$$

所以$an=na$。这样，N的两个元e和n都可以和G的任何元a交换，所以N属于G的中心。

2. 证明，两个不变子群的交集还是不变子群。

解 令N_1和N_2是群G的两个不变子群。那么$N_1\cap N_2$，是G的一个子群（§8，习题2）。我们进一步证明，$N_1\cap N_2$是G的一个不变子群。令$a\in G$，$n\in N_1\cap N_2$，那么$n\in N_1$，$n\in N_2$。但N_1和N_2是不变子群，所以$ana^{-1}\in N_1$，$ana^{-1}\in N_2$，因而

$$ana^{-1}\in N_1\cap N_2$$

于是由定理2，$N_1\cap N_2$是一个不变子群。

3. 证明，指数是2的子群一定是不变子群。

解 令G是一个群而N是G的一个指数为2的子群。

若$n\in N$，那么显然有$nN=Nn$。设$b\in G$，$b\notin N$。那么由于N的指数是2，G被分成两个左陪集N和bN；G也被分成两个右陪集N和Nb。因此$bN=Nb$。这样，对于G的任何元a来说，$aN=Na$而N是G的一个不变子群。

4. 假定H是G的子群，N是G的不变子群。证明，HN是G的子群。

解 由于H和N都不空，所以HN也不空。

设 $a \in HN$， $b \in HN$。那么

$$a = h_1 n_1, \quad b = h_2 n_2 \quad (h_1, h_2 \in H, n_1, n_2 \in N)$$

$$ab^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 n' h_2^{-1} \quad (n' = n_1 n_2^{-1})$$

由于N是一个不变子群，有

$$N h_2^{-1} = h_2^{-1} N, \quad n' h_2^{-1} = h_2^{-1} n \quad (n \in N)$$

由是得$ab^{-1} = (h_1 h_2^{-1})\, n \in HN$而$HN$是一个子群。

5. 举例证明，G的不变子群N的不变子群N_1未必是G的不变子群（取$G = S_4$）。

解 令$G = S_4$，

$$N = \{(1), (12)(34), (13)(24), (14)(23)\}$$

$$N_1 = \{(1), (12)(34)\}$$

已知N是G的一个子群（上节习题6）。我们证明，N是G的一个不变子群。为了证明这一点，我们考察，是否对一切$\pi \in S_4$，等式

$$(a) \qquad \pi N \pi^{-1} = N$$

成立。由于任何π都可以写成（$1i$）形的2-循环置换的乘积（§6．习题5），我们只须对（$1i$）形的π来看等式（a）是否成立。又由于N的元的对称性，我们只须看$\pi = (12)$的情形。但

$$(12)\{(1), (12)(34), (13)(24), (14)(23)\}(12)$$
$$= \{(1), (12)(34), (14)(23), (13)(24)\}$$

所以N是S_4的一个不变子群。由于N是交换群，N_1当然是N的一个不变子群。但N_1不是S_4的一个不变子群。因为

$(13)[(12)(34)](13)=(14)(23)\in N$；

6. 一个群G的可以写成$a^{-1}b^{-1}ab$形式的元叫作换位子。证明：

（i） 所有有限个换位子的乘积作成的集合C是G的一个不变子群；

（ii） G/C是交换群；

（iii） 若N是G的一个不变子群，并且G/N是交换群，那么

$$N\supset C$$

解 （i） C的两个元的乘积仍是有限个换位子的乘积，因而仍是C的一个元。一个换位子的逆仍是一个换位子，所以C的一个元的逆仍是C的一个元。这样C是一个子群。

对于$a\in G$，$c\in C$，$aca^{-1}=(aca^{-1}c^{-1})c\in C$，所以$C$是$G$的一个不变子群。

（ii） 令a，$b\in G$。那么$a^{-1}b^{1}ab=c\in C$。由此得

$$ab=bac,\quad abC=bacC=baC$$

即$aCbC=bCaC$而G/C是交换群。

（iii） 因为G/N是交换群，所以对G的任何两个元a和b

$$(aN)(bN)=(bN)(aN),\quad abN=baN$$

由此得 $ab=ban\quad(n\in N)\quad a^{-1}b^{-1}ab=n\in N$。

这样N含有一切换位子，因而含有C。

补充题． 令π和$(i_1i_2\cdots i_k)$属于S_n。证明

$$\pi^{-1}(i_1i_2\cdots i_k)\pi=(i_1^{\pi}\ i_2^{\pi}\ \cdots i_k^{\pi})$$

§11. 同态与不变子群

1. 我们看一个集合A到集合$\overline{A}$的满射Φ。证明，若A的子集S是$\overline{A}$的子集$\overline{S}$的逆象，$\overline{S}$一定是S的象；但若$\overline{S}$是S的象，S不一定是$\overline{S}$的逆象。

解 (i) 设S是$\overline{S}$的逆象。这时对任一元$a\in S$，存在元$\overline{a}\in\overline{S}$，使$\Phi(a)=\overline{a}$，因此$\Phi(S)\subset\overline{S}$。反过来，对任一元$\overline{a}\in\overline{S}$，存在$a\in S$，使$\Phi(a)=\overline{a}$，因此$\overline{S}\subset\Phi(S)$。这样$\overline{S}=\Phi(S)$，即$\overline{S}$是$S$的象。

(ii) 令$A=\{1, 2, 3, 4\}$，$\overline{A}=\{2, 4\}$，A到$\overline{A}$的满射是

$$\Phi:\quad 1\to 2,\quad 2\to 2,\quad 3\to 4,\quad 4\to 4$$

取$S=\{1, 3\}$。那么S的象$\overline{S}=\{2, 4\}$。但$\overline{S}$的逆象是$A\neq S$。

2. 假定群G与群$\overline{G}$同态，$\overline{N}$是$\overline{G}$的一个不变子群，N是$\overline{N}$的逆象。证明，$G/N\cong\overline{G}/\overline{N}$。

解 设所给G到$\overline{G}$的同态满射是

$$\Phi:\quad a\to\overline{a}=\Phi(a)$$

我们要建立一个G/N到$\overline{G}/\overline{N}$的同构映射。定义

$$\Psi:\quad aN\to\overline{a}\,\overline{N}$$

若$aN=bN$，那么$b^{-1}a\in N$。由于$\overline{N}$是N在Φ之下的象，有

$$\overline{b^{-1}a}=\overline{b}^{-1}\overline{a}\in\overline{N},\qquad \overline{a}\,\overline{N}=\overline{b}\,\overline{N}$$

所以Ψ是G/N到$\overline{G}/\overline{N}$的一个映射。

设$\overline{a}\overline{N} \in \overline{G}/\overline{N}$而$\Phi(a)=\overline{a}$，那么

$$\Psi: \quad aN \to \overline{a}\overline{N}$$

所以Ψ是G/N到$\overline{G}/\overline{N}$的一个满射。

若$aN \neq bN$，那么$b^{-1}a \notin N$。由于N是$\overline{N}$的逆象，由此得

$$\overline{b^{-1}a}=\overline{b}^{-1}\overline{a} \notin \overline{N}, \quad \overline{a}\overline{N} \neq \overline{b}\overline{N}$$

所以Ψ是G/N与$\overline{G}/\overline{N}$间的一个一一映射。

最后，由于

$$\Psi: \quad aNbN = abN \longrightarrow \overline{ab}\overline{N} = \overline{a}\overline{N}\overline{b}\overline{N}$$

Ψ是G/N与$\overline{G}/\overline{N}$间的一个同构映射。

3. 假定G和$\overline{G}$是两个有限循环群，它们的阶各是m和n。证明，G与$\overline{G}$同态，当而且只当$n \mid m$的时候。

解 设G与$\overline{G}$同态，那么由定理2，$G/N \cong \overline{G}$，这里N是G到$\overline{G}$的同态满射的核。所以G/N的阶是n。但G/N的阶等于不变子群N在G里的指数，所以由§9的定理2它能整除G的阶m。由此得$n \mid m$。

反过来设$n \mid m$。令$G=(a)$，$\overline{G}=(\overline{a})$。定义

$$\Phi: \quad a^k \longrightarrow \overline{a}^k$$

若$a^h=a^k$，那么$m \mid h-k$。于是由$n \mid m$，得$n \mid h-k$而$\overline{a}^h=\overline{a}^k$。这样$\Phi$是$G$到$\overline{G}$的一个映射。容易证明，$\Phi$是$G$到$\overline{G}$的一个同态满射。因此$G$与$\overline{G}$同态。

4. 假定G是一个循环群，N是G的一个子群。证明，G/N也是循环群。

解 循环群G是交换群，所以G的子群N是不变子群，而G/N有意义。

设$G=(a)$。容易证明$G/N=(aN)$。所以G/N 也是循环群。

第三章　环与域

§1. 加群、环的定义

1. 证明，本节内所给的加群的一个非空子集作成一个子群的条件是充分而且必要的。

解　可以象证明p.62定理1那样完全类似地加以证明，这里从略。

2. $R=\{0,\ a,\ b,\ c\}$，加法和乘法由以下两个表给定：

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\times$	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

证明，R作成一个环。

解　由加法表容易看出，R 对于加法来说，与克莱因四元群（参看第二章§9习题6）同构。因此R对于加法来说作成一个加群。

R 的乘法满足结合律：

$$(xy)\ z=x(yz) \qquad x,\ y,\ z\in R$$

因为当$x=0$或a时，$(xy)z=x(yz)=0$，当$x=b$或c时，$(xy)z=x(yz)=yz$。

两个分配律也都成立：

(1) $$x(y+z)=xy+xz$$

(2) $$(y+z)x=yx+xz$$

(1) 容易验证：当$x=0$或a时

$$x(y+z)=xy+xz=0$$

当$x=b$或c时

$$x(y+z)=xy+xz=y+z$$

现在分几种情形来验证（2）。

当y和z中有一个为0时，（2）显然成立。

当$y\neq0$，$z\neq0$，但 $y=z$时，由于R的任何元的两倍都等于0，所以（2）也成立。

当$y\neq0$，$z\neq0$，$y\neq z$时，有

$$(a+b)x=cx=x \qquad ax+bx=0+x=x$$

$$(b+c)x=ax=0 \qquad bx+cx=x+x=0$$

$$(c+a)x=bx=x \qquad cx+ax=x+0=x$$

由于加法满足交换律，我们已经验算了所有情形。因此（2）也成立。

这样R作成一个环。

§2. 交换律、单位元、零因子、整环

1. 证明，二项式定理

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\cdots+b^n$$

在交换环中成立。

解 对n用归纳法。当$n=1$时定理成立。设当$n=k$时定理成立：

$$(a+b)^k = a^k + \binom{k}{1}a^{k-1}b + \cdots + b^k$$

现在看 $n = k+1$的情形. 由于乘法满足交换律，有

$$(a+b)^{k+1} = [a^k + \binom{k}{1}a^{k-1}b + \cdots + b^k](a+b)$$

$$= a^{k+1}[\binom{k}{1}+1]a^k b + \cdots + [\binom{k}{i} + \binom{k}{i-1}]a^{k-i+1}b^i + \cdots + b^{k+1}$$

由于 $\binom{k}{i} + \binom{k}{i-1} = \binom{k+1}{i}$ 有

$$(a+b)^{k+1} = a^{k+1} + \binom{k+1}{1}a^k b + \cdots + \binom{k+1}{i}a^{k+1-i}b^i + \cdots + b^{k+1}$$

所以二项式定理在交换环中成立。

2. 假定一个环 R 对于加法来说作成一个循环群. 证明，R 是交换环。

解 设R 作为加群是由元 a 生成的循环群。令 b 和 c 是 R 的任意两个元，那么

$$b = ma, \qquad c = na \qquad m\text{和}n\text{是整数}$$

易见$bc = (mn)a^2 = cb$，因而 R 是交换环。

3. 证明，对于有单位元的环来说，加法适合交换律是环定义里其它条件的结果（利用$(a+b)(1+1)$）.

解 令 a 和 b 是 R 的任意两个元。由两个分配律得

$$(a+b)(1+1) = (a+b)\cdot 1 + (a+b)\cdot 1 = a+b+a+b$$

$$= a(1+1) + b(1+1) = a+a+b+b$$

于是有

$$(-a)+a+b+a+b+(-b) = (-a)+a+a+b+b+(-b)$$

$$b+a = a+b$$

这样就推出了加法适合交换律。

4. 找一个我们还没有提到过的有零因子的环。

解 令$R = \{(a,\ b,\ ),a,\ b\text{是整数}\}$。并且定义

$$(a, b) = (c, d) \quad \text{当且仅当 } a = c, \; b = d$$

进一步定义

$$(a, b) + (c, d) = (a+c, b+d)$$

$$(a, b)(c, d) = (ac, bd)$$

这显然是R的两个代数运算．由整数环的性质容易证明，R对于如上定义的加法和乘法作成一个环，而$(0, 0)$是R的零元．当$a \neq 0$，$b \neq 0$时

$$(a, 0) \neq (0, 0), \qquad (0, b) \neq (0, 0)$$

但$(a, 0)(0, b) = (0, 0)$．所以R有零因子．

5． 证明，由所有实数$a+b\sqrt{2}$（a，b是整数）作成的集合R对于普通加法和乘法来说是一个整环．

解 当a，b，c，d是整数时，

$$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$$

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$$

这里$(a+c)$，$(b+d)$，$(ac+2bd)$，$(ad+bc)$仍是整数．

所以R对普通加法和乘法来说是闭的．

普通加法和乘法适合结合律、交换律和分配律．

$$(0+0\sqrt{2}) = 0 \in R$$

对任何$a+b\sqrt{2} \in R$，有$-a-b\sqrt{2} \in R$，且

$$(a+b\sqrt{2}) + (-a-b\sqrt{2}) = 0$$

所以R作成一个交换环，又$1+0\sqrt{2} = 1 \in R$，两个非零实数的乘积不等于零．

所以R是一个整环．

§3．除环、域

1． $F = \{$所有复数$a+bi$（a，b是有理数）$\}$，证明，

F 对普通加法和乘法来说作成一个域

解 容易证明，F 对普通加法和乘法来说作成一个整环。（参看前一节习题5．）

设 $a+bi$ 是 F 的一个非零元．那么 a 和 b 不能都等于零，因而 $a^2+b^2\neq 0$．容易算出，

$$(a+bi)\left(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\right)=1$$

$$\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\in F$$

这样，F 的任意非零元在 F 中有逆而 F 是一个域．

2． $F=\{$所有实数$a+b\sqrt{3}$（a，b是有理数）$\}$．证明，F 对于普通加法和乘法来说是一个域．

解 容易证明，F 对普通加法和乘法来说作成一个整环．设 $a+b\sqrt{3}$ 是 F 的任一非零元．那么 a 和 b 不能都等于零，此时 $a^2-3b^2\neq 0$．否则将有 $a^2=3b^2$．若 $b=0$，将得 $a=0$，与假设矛盾；若 $b\neq 0$，将有 $\frac{a}{b}=\sqrt{3}$，与 $\frac{a}{b}$ 是有理数矛盾．容易算出

$$(a+b\sqrt{3})\left(\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\right)=1$$

$$\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\in F$$

这样 F 的任意非零元在 F 中有逆而 F 是一个域．

3． 证明，一个至少有两个元而且没有零因子的有限环

R是一个除环。

解 令$R^* = \{R$的一切非零元$\}$。那么因为R至少有两个元而R^*不空。并且

Ⅰ 由于R没有零因子，所以R^*对乘法来说是闭的。

Ⅱ 乘法对R的元适合结合律，对R^*的元当然也适合。

Ⅲ 由于R没有零因子，所以消去律对R^*的元成立。

但R^*只有有限个元，所以R^*作成一个乘群。

令1是R^*的单位元，那么由于$1 . 0 = 0 . 1 = 0$，1也是R的单位元，因此R^*的元在乘群R^*中的逆也是它在R中的逆。

这样R是一个除环。

4. 证明，例3的乘法适合结合律。

解 通过简单计算即可以证明，此处从略。

5. 验证，四元数除环的任意元$(a+bi,\ c+di)$，这里a, b, c, d是实数，可以写成

$$(a,\ 0)+(b,\ 0)(i,\ o)+(c,\ 0)(0,\ 1)+(d,\ 0)(0,\ i)$$

的形式。

解
$$(b,0)(i,\ 0)=(bi,\ 0)$$
$$(c,\ 0)(0,\ 1)=(0,\ c)$$
$$(d,\ 0)(0,\ i)=(0,\ di)$$

所以

$$\begin{aligned}(a,0)+(b,0)(i,0)+(c,0)(0,1)+(d,\ 0)(0,i)\\ =(a,0)+(bi,\ 0)+(0,\ c)+(0,\ di)\\ =(a+bi,\ c+di)\end{aligned}$$

§ 4. 无零因子环的特征

1. 假定F是一个有 4 个元的域. 证明:

(a) F的特征是 2;

(b) F的$\neq 0$或 1 的两个元都适合方程$x^2=x+1$.

解 (a) F的特征是F的非零元的(对加法来说的)相同的阶, 并且是一个素数. F作为加群的阶是 4, 因此F的非零元(对加法来说)的阶只能是 1, 2 或 4 其中只有 2 是素数. 所以F的特征是 2.

因此加群F与克莱因四元群B_4同构. (参看第二章§9 习题 6.)

(b) 另一方面乘群F^*的阶是 3, 因而是一个循环群(a), 而F^*的元是$1, a, a^2$.

这样$F=\{0, 1, a, a^2\}$. 由于加群F与B_4同构, 有

$$a+1=a^2 \qquad a^2+1=a=(a^2)^2$$

因此F的$\neq 0$或 1 的两个元a和a^2都适合方程$x^2=x+1$.

2. 假定$[a]$是模n的一个剩余类. 证明, 若a同n互素, 那么所有$[a]$的数都同n互素. (这时我们说$[a]$同n互素].)

解 令b属于模n的剩余类$[a]$, 那么

$$n \mid a-b \qquad a-b=ng$$

$$(1) \qquad a=b+ng$$

若$(b, n)\neq 1$, 那么b和n有公因子$m>1$, 于是m整除(1)式的右端, 因而也整除(1)式的左端: $m \mid a$. 这样, $(a, n)\neq 1$, 与假设矛盾. 这就证明了, b同n互

素。

3. 证明，所有同 n 互素的模 n 的剩余类对于剩余类的乘法来说作成一个群。（同 n 互素的剩余类的个数普通用符号 $\varphi(n)$ 来表示，并且把它叫作尤拉 φ 函数。）

解 令 $G=\{$所有同 n 互素的模 n 的剩余类$\}$。

若整数 a 和 b 都同 n 互素，那么 ab 也同 n 互素。因此，若是 $[a]\in G$，$[b]\in G$，那么 $[a][b]\in G$，即 G 对剩余类乘法是闭的。

剩余类乘法适合结合律。

由 $(1, n)=1$ 得 $[1]\in G$ 而 G 有单位元 $[1]$。

设 $[a]\in G$。那么 $(a, n)=1$，因而存在整数 s 和 t，使

$$(1) \qquad as+nt=1$$

于是 $[a][s]+[n][t]=[1]$，但 $[n]=[0]$，所以 $[a][s]=[1]$。由（1）式显然有 $(s, n)=1$，所以 $[s]\in G$。即 G 的任何元 $[a]$ 在 G 中有逆。

这样，G 作成一个群。

4. 证明，若是 $(a, n)=1$，那么 $a^{\varphi(n)}\equiv 1\ (n)$。（费马定理。）

解 上题中群 G 的阶是 $\varphi(a)$，而 $[a]\in G$，因此

$$[a]^{\varphi(n)}=[a^{\varphi(n)}]=[1] \text{ 而 } a^{\varphi(n)}\equiv 1\ (n)$$

§5. 子环、环的同态

1. 证明，一个环的中心是一个交换子环。

解 证明很容易，此处从略。

2. 证明，一个除环的中心是一个域。

解　由上题已知一个除环D的中心Z是一个交换子环。由于Z含有单位元$1 \neq 0$，要证明Z是一个域，只须证明，若非零元$z \in Z$，那么$z^{-1} \in Z$。由$0 \neq z \in Z$得

$$az = za \qquad \text{对一切 } a \in D$$

由此得$z^{-1}azz^{-1} = z^{-1}zaz^{-1}$，$z^{-1}a = az^{-1}\ (a \in D)$，即$z^{-1} \in Z$。

3.　证明，有理数域Q是所有复数$a + bi$（a，b是有理数）作成的域$Q(i)$的唯一的真子域。

解　由§3习题1知$Q(i)$是一个域。

Q显然是$Q(i)$的一个真子域。

设F是$Q(i)$的任一子域。那么F含有元$a \neq 0$，因而含有元$a^{-1}a = 1$。由此得F含有一切整数和一切有理数，因而含有Q：

$$Q \subset F \subset Q(i)$$

若$F \neq Q$，那么至少有一个数

$$a + bi \in F, \qquad a, b \in Q, \qquad b \neq 0$$

于是$a + bi - a = bi \in F$，$b^{-1}bi = i \in F$。由此得，F含有一切$a + bi$而$F = Q(i)$。

所以Q是$Q(i)$的唯一的真子域。

4.　证明，$Q(i)$有而且只有两个自同构映射。

解　设Φ是$Q(i)$的一个自同构。那么必然有

$$\Phi(0) = 0, \quad \Phi(1) = 1, \quad \Phi\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right), \quad \frac{p}{q}\text{有理数}$$

考察i的象$\Phi(i)$，由

$$-1 = \Phi(-1) = \Phi(i^2) = [\Phi(i)]^2$$

得$\Phi(i) = \pm i$。因此$Q(i)$的自同构只能是

Φ_1:　　　　　$a+bi \longrightarrow a+bi$

Φ_2:　　　　　$a+bi \longrightarrow a-bi$

容易验证，Φ_1和Φ_2的确是$Q(i)$的自同构。

因此$Q(i)$只有两个自同构。

5. J_3表示模3的剩余类所作成的集合。找出加群J_3的所有自同构映射；再找出域J_3的所有自同构映射。

解 设Φ是加群$J_3=\{[0],[1],[2]\}$的一个自同构。那么必有$\Phi[0]=[0]$。因此加群J_3的自同构只能是

Φ_1:　$[0] \longrightarrow [0]$，$[1] \longrightarrow [1]$，$[2] \longrightarrow [2]$

Φ_2:　$[0] \longrightarrow [0]$，$[1] \longrightarrow [2]$，$[2] \longrightarrow [1]$

Φ_1显然是加群J_3的一个自同构。容易验证，Φ_2也是加群J_3的一个自同构。这样，加群J_3一共有Φ_1，Φ_2这两个自同构。

设Ψ是域J_3的一个自同构。那么必有

$$\Psi[0]=[0], \qquad \Psi[1]=[1]$$

因而也必有$\Psi[2]=[2]$。这样的Ψ显然是域J_3的一个自同构。因此域J_3只有Ψ这个自同构。

6. 从略。

§6. 多项式环

1. 证明，假定R是一个整环，那么R上的一元多项式环$R[x]$也是一个整环。

解 已知$R[x]$是一个有单位元的交换环。要证$R[x]$是一个整环，只须证明，$R[x]$没有零因子。

设$f(x)$，$g(x)\in R[x]$，$f(x)\neq 0$，$g(x)\neq 0$。

那么$f(x)$和$g(x)$可以写成

$$f(x)=a_0+a_1x+\cdots+a_mx^m \quad (a_i\in R)$$
$$g(x)=b_0+b_1x+\cdots+b_nx^n \quad (b_i\in R)$$

的形式，这里$a_m\neq 0$，$b_n\neq 0$。于是

$$f(x)g(x)=c_0+c_1x+\cdots+a_mb_nx^{m+n} \ (c_i\in R)$$

但a_m，$b_n\in R$而R无零因子，所以$a_mb_n\neq 0$而

$$f(x)g(x)\neq 0$$

这样，$R[x]$没有零因子。

2. 假定R是模7的剩类环。在$R[x]$里把乘积

$$([3]x^3+[5]x-[4])([4]x^2-x+[3])$$

计算出来。

解 $([3]x^3+[5]x-[4])([4]x^2-x+[3])$

$$=[5]x^5-[3]x^4+x^3+[5]x-[5]$$

3. 证明：

(i) $R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$

(ii) 若x_1，x_2，…，x_n是R上的无关未定元，那么每一个x_i都是R上的未定元。

解 (i) 由$R[\alpha_1,\alpha_2]$的定义，$\alpha_1\alpha_2=\alpha_2\alpha_1$。设

$$f(\alpha_1,\alpha_2)\in R[\alpha_1,\alpha_2]$$

那么

$$f(\alpha_1,\alpha_2)=\sum_{i_1i_2}a_{i_1i_2}\alpha_1^{i_1}\alpha_2^{i_2}$$
$$=\sum_{i_1i_2}a_{i_1i_2}\alpha_2^{i_2}\alpha_1^{i_1}\in R[\alpha_2,\alpha_1]$$

因此$R[\alpha_1,\alpha_2]\subset R[\alpha_2,\alpha_1]$。同理$R[\alpha_2,\alpha_1]\subset R[\alpha_1,\alpha_2]$。由最后两式得$R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$。

(ii) 设某一x_i，例如x_1，不是R上的未定元，那么存在不全为0的a_1，a_2，…，$a_k \subset R$，使

$$a_0 + a_1 x_1 + \cdots + a_k x_1^k = 0$$

这个式子可以改写成

$$a_0 + a_1 x_1 x_2^0 \cdots x_n^0 + \cdots + a_k x_1^k x_2^0 \cdots x_n^0 = 0$$

这与x_1, x_2，…，x_n是R上无关未定元的题设矛盾。

4. 证明：

(i) 若是x_1，x_2，…，x_n和y_1，y_2，…，y_n是R上两组无关未定元，那么

$$R[x_1, x_2, \cdots, x_n] \cong R[y_1, y_2, \cdots, y_n) .$$

(ii) R上的一元多项式环$R[x]$能与它的一个真子环同构。

解 (i) 对$R[x_1, x_2, \cdots, x_n]$的任一元$f(x_1, x_2 \cdots, x_n)$规定

Φ: $\qquad f(x_1, x_2, \cdots, x_n) \to$

$$f(y_1, y_2, \cdots, y_n) \in R[y_1, y_2, \cdots, y_n]$$

我们证明，Φ是$R[x_1, x_2, \cdots, x_n]$与$R[y_1, y_2, \cdots y_n]$间的一个同构映射。由于$R[x_1, x_2, \cdots x_n]$的每一元只能用一种方法写成R上的多项式$f(x_1, x_2, \cdots, x_n)$，所以Φ是一个映射。由于$R[y_1, y_2, \cdots, y_n]$的元也只能用一种方式写成R上的多项式$f(y_1, y_2, \cdots, y_m)$，所以Φ是一个单射，容易看出，Φ也是满射，并且是一个同构映射。

(ii) x^2显然也是R上的一个未定元，并且由(i)

$$R[x^2] \cong R[x]$$

但$R[x^2] \subset R[x]$并且显然$x \overline{\in} R[x^2]$，因此$R[x^2]$是$R[x]$的一个真子集。

§7. 理 想

1. 假定R是偶数环。证明，所有整数$4r(r\in R)$是R的一个理想$\mathfrak{A}$。等式$\mathfrak{A}=(4)$对不对？

解 令$4r_1$，$4r_2$是$\mathfrak{A}$的任意两个元。由于偶数减偶数还是偶数，所以

$$4r_1-4r_2=4(r_1-r_2)\in\mathfrak{A}$$

令r是R的任意元。由于偶数乘偶数还是偶数，所以

$$r(4r_1)=(4r_1)r=4(r_1r)\in\mathfrak{A}$$

因此$\mathfrak{A}$是R的一个理想。

由于$4\in(4)$而$4\bar{\in}\mathfrak{A}$，所以$\mathfrak{A}\neq(4)$。

2. 假定R是整数环。证明，$(3, 7)=(1)$。

解 由于$(3, 7)$是R的理想，所以$(3, 7)$含$3.2=6$以及$7-6=1$而$(1)\subset(3, 7)$。但$(1)=R$，所以$(3.7)\subset(1)$。因此

$$(3, 7)=(1)$$

3. 假定例3的R是有理数域。证明，这时$(2, x)$是一个主理想。

解 若R是有理数域，那么$R[x]$含有有理数$\frac{1}{2}$，因而它的理想$(2, x)$含有$\frac{1}{2}2=1$。因此$(2, x)$等于主理想(1)。

4. 证明，两个理想的交集还是一个理想。

解 从略。

5． 找出模 6 的剩余类环R的所有理想。

解 $R=\{[0],[1],[2],[3],[4],[5]\}$。若$\mathfrak{A}$是$R$的一个理想，那么$\mathfrak{A}$一定是加群$R$的一个子群．但加群$R$是循环群，所以它的子群一定也是循环群，我们有

$G_1=([0])=\{[0]\}$

$G_2=([1])=\{[5]\}=R$

$G_3=([2])=\{([4])=\{[0],[2],[4]\}$

$G_4=([3])=\{[0],[3]\}$

易见，G_1，G_2，G_3，G_4都是R的理想，因而是R的所有理想．

6． 一个环R的一个非空子集S叫作R的一个左理想，假如

(i) $\qquad a, b\in S\longrightarrow a-b\in S$

(ii) $\qquad a\in S, r\in R\longrightarrow ra\in S$

你能不能在有理数域F上的2×2矩阵环F_{22}里找到一个不是理想的左理想？

解 令S是由有理数域上一切形如

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

的矩阵组成的。易见

$A, B\in S\Longrightarrow A-B\in S,$

$A\in S, L\in F_{22}\Longrightarrow LA\in S$

所以S是F_{22}的一个左理想．若取

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\in S \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\in F_{22}$$

那么

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\notin S$$

所以 S 不是 F_{22} 的一个理想。

§8. 剩余类环、同态与理想

1． 假定我们有一个环 R 的一个分类，而 S 是由所有的类 $[a]$，$[b]$，$[c]$，…所作成的集合。

又假定

$$[x]+[y]=[x+y] \qquad [x][y]=[xy]$$

规定两个 S 的代数运算。证明，$[0]$ 是 R 的一个理想，并且给定的类刚好是模 $[0]$ 的 R 的剩余类。

解 设 u，$v\in[0]$，$r\in R$。那么 $[u]=[v]=[0]$。

$$[u-v]=[u]-[v]=[0]-[0]=[0]$$

$$[ru]=[r][u]=[r][0]=[0]$$

$$[ur]=[u][r]=[0][r]=[0]$$

因此 $u-v\in[0]$，$ru\in[0]$，$ur\in[0]$，而 $[0]$ 是 R 的一个理想。

设 $[u]=[v]$。那么 $[u]-[v]=[u-v]=[0]$ 而 $u-v\in[0]$。反之，设 $u-v\in[0]$，那么

$$[u]-[v]=[u-v]=[0] \text{而} [u]=[v]。$$

所以 $[u]=[v]$ 当而且仅当 $u-v\in[0]$ 的时候，这就是说，给定的类刚好是模 $[0]$ 的 R 的剩余类。

2． 假定 Φ 是环 R 到环 $\overline{R}$ 的一个同态满射。证明，Φ 是 R 与 $\overline{R}$ 间的同构映射，当而且只当 Φ 的核是 R 的零理想的时候。

解 设 $\Phi(a)=\overline{a}$ $(a\in R,\ \overline{a}\in\overline{R})$。若 Φ 是一个同构映射，那么 Φ 是一个一一映射，因而在 Φ 之下，只有 R

的零元 0 是$\overline{R}$的零元$\overline{0}$的逆象，这就是说，Φ的核是R的零理想$\{0\}$。

反过来，设Φ的核是R的零理想$\{0\}$。那么R的任何一个元$c\neq 0$的象$\overline{c}\neq 0$。因此由$a\neq b$ $(a, b\in R)$ 得

$$0\neq a-b\longrightarrow \overline{a}-\overline{b}\neq \overline{0}$$

即$\overline{a}\neq\overline{b}$而$\Phi$是一个同构映射。

3. 假定R是由所有复数$a+bi$(a，b是整数）作成的环。环$R/(1+i)$有多少个元？

解 先看R的主理想$(1+i)$含有哪些元。

设 $a+bi\in(1+i)$。那么

$$a+bi=(x+yi)(1+i)=(x-y)+(x+y)i$$

因此，若x和y同为奇数或同为偶数，那么a和b同为偶数；若x和y一奇一偶，那么a和b同为奇数。这样，a和b必须有相同的奇偶性。反过来，设a和b有相同的奇偶性，那么方程组

$$x-y=a \qquad x+y=b$$

有整数解$x=\dfrac{a+b}{2}$，$y=\dfrac{b-a}{2}$因而$a+bi\in(1+i)$。

这样，当且仅当a和b有相同的奇偶性时，

$(a+bi)\in(1+i)$。此时$[a+bi]=[0]$

现在设a和b一奇一偶，那么

$$(a+bi)=1+[(a-1)+bi]$$

而$a-1$和b有相同的奇偶性。这时

$$a+bi=1+u \qquad u\subset(1+i)$$

而$[a+bi]=[1]$，因此环$R/(1+i)$含两个元素$[0]$和$[1]$。

§9. 最大理想

1. 假定R是由所有复数$a+bi(a, b$是整数) 所作成的环. 证明, $R/(1+i)$是一个域。

解 只须证明, $(1+i)$是R的一个最大理想. 设$\mathfrak{A}$是R的一个理想, 并且

$$(1+i) \subset \mathfrak{A} \subset R \qquad (1+i) \neq \mathfrak{A}$$

根据这一假设, 由前一节习题3, $\mathfrak{A} \ni a+bi$, 此处a和b一奇一偶, 因而主理想$(a+bi) \ni 1$, 这样$\mathfrak{A} \ni 1$而$\mathfrak{A}=R$.

另一解法, 容易看出$R/(1+i)$与模2的剩余类环同构。因此, 由于2是一个素数, $R/(1+i)$是一个域。

2. 我们看环R上的一个一元多项式环$R[x]$。当R是整数环时, $R[x]$的主理想(x)是不是一个最大理想? 当R是有理数域时, 情形如何?

解 考察$R[x]$的理想$(2, x)$. 由于(x)的元都可以写成$f(x)x$的形式, 此处$f(x) \in R[x]$, 所以显然有

$$(x) \subset (2, x), \qquad 2 \overline{\in} (x), \qquad (x) \neq (2, x)$$

当R是整数环时, 由§7例3, $(2, x)$不是一个主理想, 因而

$$(2, x) \neq (1) = R[x].$$

因此(x)不是一个最大理想。

当R是有理数域时, 设$\mathfrak{A}$是$R[x]$的一个理想, 并且

$$(x) \subset \mathfrak{A} \qquad (x) \neq \mathfrak{A}$$

那么

$$\mathfrak{A} \ni f(x) = a_0 + a_1x + \cdots + a_nx^n, \qquad a_0 \neq 0$$

由此得

$$\mathfrak{A} \ni f(x) - x(a_1 + a_2 x + \cdots + a_n x^{n-1}) = a_0$$

因此 $\mathfrak{A} \ni \frac{1}{a_0} a_0 = 1$ 而 $\mathfrak{A} = (1) = R[x]$。这就是说，在这一情形 (x) 是一个最大理想。

3. 我们看所有偶数作成的环 R。证明，(4) 是 R 的一个最大理想，但 $R/(4)$ 不是一个域。

解 (4) 刚好含有一切 $4n$，这里 n 是整数。设 $\mathfrak{A}$ 是 R 的一个理想，并且 $(4) \subset \mathfrak{A}$，$(4) \neq \mathfrak{A}$。那么

$$\mathfrak{A} \ni a = 2m \neq 4n$$

由此 $a = 4q + 2$，$\mathfrak{A} \ni 4q + 2 - 4q = 2$ 而 $\mathfrak{A} = (2) = R$

这就是说，(4) 是 R 的一个最大理想。

在 $R/(4)$ 中，$[2] \neq [0]$ 而 $[2][2] = [4] = [0]$。因此 $R/(4)$ 有零因子因而不是一个域。

4. 我们看有理数域 F 上的全部 2×2 矩阵环 F_{22}。证明，F_{22} 只有零理想和单位理想，但不是一个除环。

解 设 $\mathfrak{A}$ 是 F_{22} 的一个理想并且 $\mathfrak{A} \neq \{0\}$。那么 $\mathfrak{A}$ 含有 2 阶矩阵 $A \neq 0$。

若 A 的秩是 2，那么 A 有逆 A^{-1} 而

$$A^{-1}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E \in \mathfrak{A}$$

此时 $\mathfrak{A} = (E) = F_{22}$。

若 A 的秩等于 1，则存在初等矩阵 P 和 Q，使

$$PAQ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{A}$$

容易算出

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&0\\0&1\end{pmatrix}\in\mathfrak{A}$$

因此$\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}=E\in\mathfrak{A}$而也有，$\mathfrak{A}=(E)=F_{22}$。这就是说，$F_{22}$只有零理想和单位理想。

但

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

所以F_{22}有零因子而不是一个除环。

§10. 商　域

1. 证明，一个域F是它自己的商域。

解　由于$F\subset F$，所以根据定理3 F含有一个F的商域Q：$Q\subset F$。但由商域的定义，有$F\subset Q$。所以$F=Q$而F是它自己的商域。

2. 详细证明本节定理3。

解　我们只须证明，在定理的证明中所做的$\bar{Q}$是域F的一个子域。

由于$\bar{Q}$是F的一个子集，$\bar{Q}$的加法和乘法是

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

$$\frac{a}{b}\,\frac{c}{d}=\frac{ac}{bd}$$

我们按照p.97所列的条件来验证$\bar{Q}$是F的一个子域。

$\bar{Q}$包含$\frac{a}{a}=1$，所以$\bar{Q}$包含一个不等于零的元。

$$\frac{a}{b},\ \frac{c}{d}\in \bar{Q}\Longrightarrow \frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}\in \bar{Q}$$

$$\frac{a}{b},\ \frac{c}{d}\in \bar{Q},\ \frac{c}{d}\neq 0\Longrightarrow \frac{a}{b}\left(\frac{c}{d}\right)^{-1}=\frac{a}{b}\ \frac{d}{c}$$

$$=\frac{a\ d}{b\ c}\in \bar{Q}$$

第四章　整环里的因子分解

§1. 素元、唯一分解

1. 证明，0不是任何元的真因子。

解 若0是元a的因子，那么$a=0.c=0$。但$0=\varepsilon.0$（ε是单位），所以0是0的相伴元。因此0不是$a(=0)$真因子。

2. 我们看以下的整环I：I刚好包含所有可以写成

(a)　　$\frac{m}{2^n}$　（m是任意整数，n是$\geqslant 0$的整数）形式

的有理数。I的哪些个元是单位，哪些个元是素元？

解 I的元总可以写成

(a)　　$2^i u$　（i整数，u奇数）

的形式。

(i)　设$\varepsilon=2^i u$是I的一个单位。那么存在ε^{-1}，使

$$\varepsilon^{-1}2^i u=1，\text{即}\ \varepsilon^{-1}=2^{-i}u^{-1}$$

于是由于I的元都有(a)的形式，必有$u=\pm 1$而$\varepsilon=\pm 2^i$。反过来，设$\varepsilon=\pm 2^i$（i整数），那么ε有逆$\varepsilon^{-1}=\pm 2^{-i}$而$\varepsilon$是$I$的单位。所以$I$的单位是一切可以写成$\pm 2^i$（$i$整数）形式的元。

(ii)　要看I的元$2^i u$是不是I的素元，由定理2只须看它的相伴元u是不是I的素元。

若奇数 u 在整数中不是素数，那么 $u=u_1u_2$，此处u_1和u_2都是不等于 ± 1 的奇数，因而由（i）都不是 I 的单位。这就是说，u 也不是 I 的素元，若奇数 u 在整数环中是一个素数而在 I 中

$$u=(2^{i_1}u_1)(2^{i_2}u_2)=2^{i_1+i_2}u_1u_2$$

此处u_1和u_2是奇数，那么必有$i_1+i_2=0$，$u=u_1u_2$。于是由于 u 是素数，u_1和u_2中必然有一个是± 1 而 $2^{i_1}u_1$ 和$2^{i_2}u_2$ 中必然有一个是 I 的单位。这就是说，u 也是I的素元。所以 I 的素元是一切可以写成2^iu，其中 u 是奇数的元。

3. I 是刚好包含所有复数

$$a+bi \qquad (a,\ b\text{是整数})$$

的整环。证明 5 不是 I 的素元。5 有没有唯一分解？

解 与本节的例完全类似，容易证明：

（i） I 的一个元 ε 是一个单位，当而且只 $|\varepsilon|^2=1$ 的时候。I 只有 4 个单位，就是 ± 1 和 $\pm i$。

(ii) 适合条件$|\alpha|^2=5$ 的 I 的元 α 一定是素元。

我们进一步证明。

(iii) 5 不是 I 的一个素元，并且 5 有唯一分解。

由于

$$(1) \qquad 5=(1+2\sqrt{2})(1-2\sqrt{2})$$

而$|1+2\sqrt{2}|^2=|1-2\sqrt{2}|^2=5$，所以根据($ii$)，(1)式给出了 5 的一个素元分解而 5 不是 I 的一个素元。设

$$(2) \qquad 5=\alpha_1\alpha_2\cdots\alpha_m$$

是 5 在 I 中的任一素元分解。那么由于 5 不是素元. $m\geqslant 2$。另一方面

$$|5|^2=25=|\alpha_1|^2|\alpha_2|^2\cdots|\alpha_m|^2$$

由于 α_i 不是单位，$|\alpha_i|^2$是不等于 1 的正整数，所以$m = 2$而（2）必是 $5 = \alpha\beta$的形式，并且$|\alpha|^2 = |\beta|^2 = 5$。由此易见，5只能有四种素元分解：

$$5 = (1+2i)(1-2i)$$

$$5 = (-1-2i)(-1+2i) = [-1(1+2i)][-1(1-2i)]$$

$$5 = (2+i)(2-i) = [i(1-2i)][-i(1+2i)]$$

$$5 = (-2-i)(-2+i) =]-i(1-2i)][i(1+2i)]$$

因此，由于 ± 1，$\pm i$都是 I 的单位，5有唯一分解。

§2. 唯一分解环

1. 证明本节的推论。

解 先证：一个唯一分解环 I 的 n 个元 a_1，a_2，…，a_n在 I 里一定有最大公因子。我们用归纳法。

当 $n = 2$ 时，由定理 3，结论成立。

设 $n = k-1$（$2 \leqslant k-1$）时，结论成立。

看 $n = k$的情形。设 a_1，a_2，…，a_{k-1}的一个最大公因子是d_1而d_1，a_k的一个最大公因子是d。那么

$$d|d_1|a_1,\ a_2,\ \cdots a_{k-1},\ d|a_k$$

所以 d 是a_1，a_2，…，a_k的一个公因子。设 c 是a_1，a_2，…，a_k的任一公因子。那么$c|a_1$，a_2，…，a_{k-1}因而$c|d_1$。于是由$c|a_k$得$c|d$。所以 d 是a_1，a_2…，a_k的一个最大公因子。这样，结论对任何 n 成立。

至于a_1，a_2，…，a_n的两个最大公因子只能差一个单位因子的证明，同定理 3 的相应证明。

2． 假定在一个唯一分解环里

$$a_1 = db_1,\ a_2 = db_2,\ \cdots,\ a_n = db_n\ （a_i\text{不全为零}）$$

证明：当而且只当 d 是 a_1，a_2，…，a_n 的一个最大公因子的时候，b_1，b_2，…，b_n 互素。

解 假定 d 不是 a_1，a_2，…，a_n 的一个最大公因子。令 c 是 a_1，a_2…，a_n 的一个最大公因子。那么 $d|c$，$c = dh$，此处 h 不是一个单位。于是对 $i = 1$，2，…，n 有

$$a_i = ck_i = dhk_i = db_i$$

由于 a_n 不全为零，得 $d \neq 0$，因而 $hk_i = b_i$，即 h 是 $b_1 b_2$，…，b_n 的一个非单位公因子。这就是说，b_1，b_2…，b_n 不互素。

假定 d 是 a_1，a_2，…a_n 的一个最大公因子。令 t 是 b_1，b_2，…，b_n 的一个公因子，那么 dt 是 a_1，a_2…，a_n 的一个公因子，因而 $dt|d$。由此得 $t|1$，而 t 是一个单位。所以 b_1，b_2，…b_n 只有单位公因子，即 b_1，b_2，…，b_n 互素。

3． 假定 I 是一个整环，(a) 和 (b) 是 I 的两个主理想。证明：$(a) = (b)$ 当而且只当 b 是 a 的相伴元的时候。

解 设 $(a) = (b)$。那么 $a \in (b)$ 所以 $a = sb$。同样有 $b = ta$，因而 $a = sta$。若 $a = 0$，那么 $b = 0$，而 b 是 a 的一个相伴元。若 $a \neq 0$，那么 $st = 1$，t 是一个单位而 b 也是 a 的一个相伴元。

设 b 是 a 的一个相伴元，那么 $b = ta$，t 是一个单位。由此得 $(b) \subset (a)$。但 $a = t^{-1}b$，所以 $(a) \subset (b)$。这样 $(a) = (b)$。

§3. 主理想环

1. 假定I是一个主理想环，并且$(a, b)=(d)$.证明：d是a和b的一个最大公因子，因此a和b的任何最大公因子d都可以写成以下形式：

$$d=sa+tb \quad (s, t\in I)$$

解 由$(a, b)=(d)$得$a\in(d)$，$b\in(d)$。因此$d|a$，$d|b$而d是a和b的一个公因子。又由$d\in(a, b)$得$d=s'a+t'b(s', t'\in I)$.因此由$c|a$和$c|d$可得$c|p$，即a和b的任何公因子c都能整除d。所以d是a和b的一个最大公因子。

若d'是a和b的任一最大公因子，那么d'是d的相伴元：$d'=\varepsilon d$（ε是I的一个单位）。因此

$$d'=\varepsilon s'a+\varepsilon t'b=sa+tb \quad (s, t\in I)$$

2. 一个主理想环I的每一个非零最大理想都是由一个素元所生成的。

解 设(a)是I的一个非零最大理想。那么由$(a)\neq I$得a不是一个单位；由(a)非零得$a\neq 0$.若a不是一个素元，那么$a=bc$，其中b是a的一个真因子。于是$(b)\supset(a)$。但由于b不是单位，$(b)\neq I$；由于b不是a的一个相伴元，$(b)\neq(a)$。这样(a)不是I的一个最大理想，与假设矛盾。

3. 我们看两个主理想环I和I_0，这里I_0是I的一个子环。假定a和b是I_0的两个元而d是这两个元在I_0里的一个最大公因子.证明：d也是这两个元在I里的一个最大公

因子。

解 由于I_0是一个主理想环，根据题1，

$$(1) \qquad d = sa + tb \qquad (s, t \in I_0)$$

在I中，d显然也是a和b的一个公因子。设c是a和b在I中的任一公因子。那么由于(1)式在I中仍然成立。c能整除(1)式的右端，因而也能整除它的左端d。这样d也是a和b在I中的一个最大公因子。

§4. 欧氏环

1. 证明，一个域F一定是一个欧氏环。

解 令N={一切$\geqslant 0$的整数}。定义

$$\Phi: \qquad a \longrightarrow 1 \qquad a \in F, \qquad a \neq 0$$

那么Φ是F^*到N的一个映射。给了F^*的一个元a，F的任何元b可以写成

$$b = (ba^{-1})\, a + 0$$

所以F是一个欧氏环。

2. 看有理数域F上的一元多项式环$F[x]$。理想

$$(x^2+1,\ x^5+x^3+1)$$

等于怎样的一个主理想？

解 由于$(x^5+x^3+1) - x^3(x^2+1) = 1$，所以

$$1 \in (x^2+1,\ x^5+x^3+1)$$

由是得$(x^2+1,\ x^5+x^3+1) = (1)$。

3. 证明，由所有复数$a+bi$(a, b是整数)所作成的环R是一个欧氏环。(取$\Phi(\alpha) = |\alpha|^2$。)

解 令N是一切$\geqslant 0$的整数作成的集合而R^*是R的一

切非零元作成的集合。定义

$$\Phi: \qquad \alpha \longrightarrow |\alpha|^2 \quad \alpha \in R^*$$

那么Φ是R^*到N的一个映射。

令$\alpha = a + bi$是R^*的一个元。那么在复数域中α有逆

$$\alpha^{-1} = \frac{a - bi}{\Phi(\alpha)}$$

令$\beta = c + di$是R的任何一元。那么$\beta = (\beta\alpha^{-1})\alpha$而

$$\lambda' = \beta\alpha^{-1} = (c + di)\left(\frac{a}{\Phi(\alpha)} - \frac{b}{\Phi(\alpha)} i\right)$$

$$= k' + l' i$$

其中k'和l'是有理数。可以找到整数k和l，使

$$|k' - k| \leqslant \frac{1}{2} \quad |l' - l| \leqslant \frac{1}{2}$$

因而

$$(k' - k)^2 \leqslant \frac{1}{4} \qquad (l' - l)^2 \leqslant \frac{1}{4}$$

令$\lambda = k + li$，那么

$$\beta = \lambda' \alpha = \lambda\alpha + (\lambda' - \lambda)\alpha = \lambda\alpha + \rho$$

由于β，$\lambda\alpha \in R$，所以$\rho \in R$，这里或者$\rho = 0$或者

$$|\rho|^2 = |\lambda' - \lambda|^2 |\alpha|^2 = [(k' - k)^2 + (l' - l)^2]|\alpha|^2$$

$$\leqslant \left(\frac{1}{4} + \frac{1}{4}\right)|\alpha|^2 < |\alpha|^2$$

即$\Phi(\rho) < \Phi(\alpha)$。所以$R$是一个欧氏环。

§5. 多项式环的因子分解

1. 假定 I 是一个唯一分解环而 Q 是 I 的商域. 证明, $I[x]$的一个多项式若是在$Q[x]$里可约, 它在 $I[x]$ 里已经可约。

解 令 $f(x)$ 是 $I[x]$的一个多项式, 并且在$Q[x]$里可约. $f(x)$ 可以写成 $f(x)=df_0(x)$, 这里 $f_0(x)$ 是 $I[x]$的一个本原多项式. 因为 d 是Q的一个单位而$f(x)$在$Q[x]$里可约, 所以$f_0(x)$在$Q[x]$里可约, 于是由引理3, $f_0(x)$ 从而$f(x)$在 $I[x]$里可约。

2. 假定$I[x]$是整环 I 上的一元多项式环, $f(x)$属于 $I[x]$但不属于I, 并且 $f(x)$的最高系数是 I 的一个单位。证明 $f(x)$ 在 $I[x]$里有分解。

解 (i) 首先以下简单事实成立: 若 a 和 b 是 I 的元, ε 是 I 的一个单位而 $ab=\varepsilon$, 那么 a 和 b 都是 I 的单位。这是因为

$$ab=\varepsilon \Longrightarrow \quad a(b\varepsilon^{-1})=1, \quad (\varepsilon^{-1}a)b=1$$

(ii) 现在证明, $f(x)$在$I[x]$里可以分解为有限个不可约多项式的乘积。若 $f(x)$本身是 $I[x]$ 的一个不可约多项式, 那么用不着再证明什么. 设 $f(x)$在$I[x]$ 里可约:

$$f(x)=g(x)h(x)$$

这里 $g(x)$和$h(x)$ 是 $f(x)$的真因子. 若$g(x)$, $h(x)$中有一个属于 I, 例如 $g(x)=a\in I$, 那么 a 与 $h(x)$的最高系数 b 的乘积等于 $f(x)$的最高系数 ε, 这里ε依照题设是 I 的一个单位. 因此由(i), a 也是 I 的一个单位, 与

a是$f(x)$的一个真因子的假设矛盾。这样$g(x)$和$h(x)$的次数都大于零因而都小于$f(x)$的次数，并且由(i)，$g(x)$和$h(x)$的最高系数都是I的单位。因此可以同样地对$g(x)$和$h(x)$进行对$f(x)$的论证。由于$f(x)$的次数有限，最后可以在$I[x]$里把$f(x)$分解为有限个不可约多项式的乘积。

§6. 因子分解和多项式的根

1. 假定R是模16的剩余类环。$R[x]$的多项式x^2在R里有多少个根？

解 x^2在R里共有4个根，即[0]，[4]，[8]，[12]。

2. 假定F是模3的剩余类环。看$F[x]$的多项式。

$$f(x)=x^3-x.$$

证明，$f(a)=0$，不管a是F的哪一个元。

解 从略。

3. 证明本节的导数规则。

解 从略。

第五章　扩域

§1. 扩域、素域

证明：$F(s)$ 的一切添加 s 的有限子集于 F 所得子域的并集 $\overline{F}$ 是一个域。

解　设 $\alpha \in F(s)$。那么

$$\alpha = \frac{f_1(\alpha_1, \alpha_2 \cdots, \alpha_n)}{f_2(\alpha_1 \alpha_2, \cdots, \alpha_n)}$$

这里 $\{\alpha_1, \alpha_2, \cdots \alpha_n\} = s_n \subset s$ 而 f_1 和 $f_2(\neq 0)$ 是 F 上 α_1，α_2，…，α_n 的多项式。由于 s_a 是 s 的一个有限子集，因此 $\alpha \in F(s_a) \subset \overline{F}$。这就是说，$F(s) \subset \overline{F}$。反过来，显然 $\overline{F} \subset F(s)$。因此 $\overline{F} = F(s)$ 而 $\overline{F}$ 是一个域。

§2. 单扩域

1. 令 E 是域 F 的一个扩域而 $\alpha \in F$。证明，α 是 F 上一个代数元，并且 $F(\alpha) = F$。

解　$f(x) = x - \alpha$　是 $F(x)$ 的一个非零多项式，并且

$$f(\alpha) = 0$$

所以 α 是 F 上的一个代数元。

由于 $F(\alpha)$ 含 F 和 α，所以 $F \subset F(\alpha)$。

由于 F 是含 F 和 α 的一个 E 的子域而 $F(\alpha)$ 是含 F 和 α 的 E 最小子域，所以 $F(\alpha) \subset F$。

这样$F(\alpha)=F$。

2. 令F是有理数域。复数i和$\frac{2i+1}{i-1}$在F上的极小多项式各是什么？$F(i)$和$F\left(\frac{2i+1}{i-1}\right)$是否同构？

解 显然$\frac{2i+1}{i-1}\in F(i)$，因而$F\left(\frac{2i+1}{i-1}\right)\subset F(i)$。另一方面

$$\left(\frac{2i+1}{i-1}\right)^2=\frac{-3}{2i}+2\in F\left(\frac{2i+1}{i-1}\right)$$

$$\left[\left(\frac{-3}{2i}+2\right)-2\right]^{-1}\left(-\frac{3}{2}\right)=i\in F\left(\frac{2i+1}{i-1}\right)$$

因而$F(i)\subset F\left(\frac{2i+1}{i-1}\right)$。这样$F(i)=F\left(\frac{2i+1}{i-1}\right)$，因而

$$F(i)\cong F\left(\frac{2i+1}{i-1}\right)$$

F上的一次多项式$f(x)=x-a$（a是有理数）显然不能满足条件$f(i)=0$，所以i在F上的极小多项式不能是一次的。但F上的二次多项式$p(x)=x^2+1$满足条件$p(i)=0$。所以i在F上的极小多项式是x^2+1。

同样$\frac{2i+1}{i-1}$在F上的极小多项式不可能是一次的。由

$$\frac{2i+1}{i-1}=\frac{(2i+1)(i+1)}{(i-1)(i+1)}=\frac{1}{2}-\frac{3}{2}i$$

容易算出，$\frac{2i+1}{i-1}$在F上的极小多项式是$x^2-x+\frac{5}{2}$。

3. 详细证明，定理3中α在域F上的极小多项式是$p(x)$。

解 令$\mathfrak{A}$是$F[x]$中一切满足条件$f(\alpha)=0$的多项式$f(x)$作成的集合。由于$p(x)\in\mathfrak{A}$，所以$\mathfrak{A}$不空。设$f(x)$，$g(x)\in\mathfrak{A}$而$h(x)\in F[x]$。那么

$$f(\alpha)=0,\ g(\alpha)=0\Longrightarrow f(\alpha)-g(\alpha)=0$$
$$\Longrightarrow f(x)-g(x)\in\mathfrak{A}$$

$$f(\alpha)=0\Longrightarrow h(\alpha)f(\alpha)=0\Longrightarrow h(x)f(x)\in\mathfrak{A}$$

所以$\mathfrak{A}$是$F[x]$的一个理想。但由于$F[x]$是一个主理想环，所以$\mathfrak{A}=(p_1(x))$。由于$\mathfrak{A}\ni p(x)\neq 0$，所以$\mathfrak{A}$不是零理想而$\psi_1(x)\neq 0$。可以假定$p_1(x)$的最高系数是1。但$\mathfrak{A}$中一切$f(x)$都能被$p_1(x)$整除，因此$p_1(x)$是$\mathfrak{A}$中次数最低的多项式，而它是$\alpha$在域$F$上的极小多项式。又由$p_1(x)\mid p(x)$而$p(x)$不可约，得$p(x)=cp_1(x)$，$c\in F$。但$p(x)$和$p_1(x)$的最高系数都是1，所以$p(x)=p_1(x)$而$p(x)$是$\alpha$在$F$上的极小多项式。

4. 证明，定理3中的$F(\alpha)=K$。

解 由于K是域F的扩域而$\alpha\in K$，所以$F(\alpha)\subset K$。

令β是K的任一元。令K与$F[x]/p(x)$间的同构映射为Φ，而β在Φ之下的象为$\overline{\beta}$。那么

$$\overline{\beta}=\overline{b}_m\overline{x}^m+\overline{b}_{m-1}\overline{x}^{m-1}+\cdots+\overline{b}_0$$

由于在同构映射Φ之下，$\bar{\beta}$的逆象是β，$\bar{b}_i$的逆象是$b_i \in F$，$i=0, 1, \cdots, m$，$\bar{x}$的逆象是α，所以

$$\beta = b_m\alpha^m + b_{m-1}\alpha^{m-1} + \cdots + b_0$$

而$\beta \in F(\alpha)$。这样反过来有$K \subset F(\alpha)$而$F(\alpha) = K$。

§3. 代数扩域

1. 令E是域F的一个代数扩域，而α是E上的一个代数元. 证明，α是F上的一个代数元。

解 因为α是域E上的一个代数元，所以存在E上的多项式，$f(x) \neq 0$，使

$$(1) \qquad f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0 \quad (a_i \in E)$$

由于E是域F的一个代数扩域，所以a_i都是F上代数元，而E的子域$E' = F(a_0, a_1, \cdots, a_n)$是$F$上一个有限扩域。但由(1)，$\alpha$显然是$E'$上一个代数元。所以$E'(\alpha)$是$E'$上一个有限扩域因而是$F$上一个有限扩域。这样

$$E'(\alpha) = F(a_0, a_1, \cdots, a_{n-1}, \alpha)$$

是F上一个代数扩域而α是F上一个代数元。

2. 令F，I和E是三个域并且$F \subset I \subset E$。假定

$$(I : F) = m$$

而E的元α在F上的次数是n，并且$(m, n) = 1$。证明，α在I上的次数也是n。

解 由于α在F上的次数是n，所以α在F上的极小多项式$p(x)$的次数是n。设α在I上的极小多项式$p_1(x)$的次数是s。那么由于$p(x)$也是I上的多项式，得$p_1(x)|$

$p(x)$而 $s\leqslant n$。设 $I(\alpha)$在$F(\alpha)$ 上的次数为 t。那么

$$(I(\alpha):F)=(I(\alpha):F(\alpha))(F(\alpha):F)=tn$$

$$(I(\alpha):F)=(I(\alpha):I)(I:F)=sm$$

因此$tn=sm$而 $n\mid sm$。但 $(m,n)=1$，所以 $n\mid s$。

由 $s\leqslant n$ 和 $n\mid s$ 得 $s=n$。这就是说，α 在 I 上的次数也是 n。

3. 令域F的特征不是2，E是F的一个扩域，并且

$$(E:F)=4$$

证明，存在一个满足条件$F\subset I\subset E$ 的F的二次扩域 I 的充分与必要条件是：$E=F(\alpha)$ 而 α 在F上的极小多项式是

$$x^4+ax^2+b$$

解 先证条件是充分的。设 $E=F(\alpha)$而 α 在F上的极小多项式是 x^4+ax^2+b。那么令 $I=F(\alpha^2)$，就显然有$F\subset I\subset E$。由于 x^4+ax^2+b 在F上不可约，所以 x^2+ax+b 在F上也不可约。但

$$(\alpha^2)^2+a(\alpha^2)+b=\alpha^4+a\alpha^2+b=0$$

所以 x^2+ax+b 是α^2 在F上的极小多项式而 I 是F的二次扩域。

现在反过来证明条件是必要的。设

$$F\subset I\subset E \qquad (I:F)=2 \qquad (E:F)=4$$

(i) 显然有 $(E:I)=2$。取$\theta\in E$，$\theta\notin I$，那么θ 在 I 上的次数是2。设θ 在 I 上的极小多项式是 $x^2+\beta x+\gamma$，那么

$$\theta^2+\beta\theta+\gamma=0 \qquad \beta,\ \gamma\in I$$

由于F的特征不是2，$\theta+\frac{\beta}{2}$有意义。我们有

$$\left(\theta+\frac{\beta}{2}\right)^2=\theta^2+\beta\theta+\frac{\beta^2}{4}+\gamma-\gamma=\frac{\beta^2}{4}-\gamma$$

令 $\omega=\theta+\frac{\beta}{2}$，$\delta=\frac{\beta^2}{4}-\gamma$，那么 $E=I(\omega)$ 而 ω 在 I 上的极小多项式是 $x^2-\delta(\delta\in I)$。

(ii) 设 $\delta\bar{\in}F$，那么 δ 在 F 上的极小多项式是

$$x^2+ax+b \quad (a,\ b\in F)$$

由于 $\omega^2=\delta$，所以 $\omega^4+a\omega^2+b=0$。但

$$I=F(\delta),\ E=I(\omega)=F(\delta,\ \omega)=F(\omega)$$

而 $(E:F)=4$，所以 ω 在 F 上的极小多项式是 x^4+ax^2+b。

(iii) 若 $\delta\in F$，那么由于 $(I:F)=2$，与（i）平行可以找到 $\lambda\in I$，$\lambda\bar{\in}F$ 而 $\lambda^2\in F$。取 $\omega'=\omega(1+\lambda)$。那么

$$\omega'^2=\omega^2(1+2\lambda+\lambda^2)$$

由于 $\omega^2=\delta\in F$ 而 $1+2\lambda+\lambda^2\bar{\in}F$，所以 $\omega'^2=\delta'\bar{\in}F$。于是与(ii) 一样有 $E=F(\omega')$ 而 ω' 在 F 上的极小多项式是

$$x^4+ax^2+b.$$

4. 令 E 是域 F 的一个有限扩域。那么总存在 E 的有限个元 α_1，α_2，…，α_m，使

$$E=F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$$

解 设 $(E:F)=m$。那么 E 作为 F 上向量空间有一组基 α_1，α_2，…，α_m。显然

$$E=F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m)$$

5. 令 F 是有理数域，看添加复数于 F 所得扩域

$$E_1=F\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}i\right)$$

$$E_2=F\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}\omega i\right),\quad \omega=\frac{-1+\sqrt{3}\,i}{2},\quad \omega^3=1$$

证明：

$$\left(E_1:F\left(2^{\frac{1}{3}}\right)\right)=2\qquad (E_1:F)=6$$

$$\left(E_2:F\left(2^{\frac{1}{3}}\right)\right)=4\qquad (E_2:F)=12$$

解 $E_1=F\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}i\right)=F\left(2^{\frac{1}{3}},\ i\right)\supset F\left(2^{\frac{1}{3}}\right)\supset F$

因为$i\overline{\in}F\left(2^{\frac{1}{3}}\right)$而$i$是$x^2+1$的根，所以$\left(E_1:F\left(2^{\frac{1}{3}}\right)\right)=2$。

因为$2^{\frac{1}{3}}\overline{\in}F$而$2^{\frac{1}{3}}$是$F$上不可约多项式$x^3-2$的一个根，所以$F\left(2^{\frac{1}{3}}\right)$是$F$上一个3次扩域。因此

$$(F_1:F)=\left(E_1:F\left(2^{\frac{1}{3}}\right)\right)\left(F\left(2^{\frac{1}{3}}\right):F\right)=2\times 3=6$$

由$E_2=F\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}\omega i\right)$得$\omega i\in E_2$，$-(\omega i)^3=i\in E_2$。

于是由$\omega=\frac{-1+\sqrt{3}}{2}i$得$\sqrt{3}\in E_2$。所以

$$E_2=F\left(2^{\frac{1}{3}},\sqrt{3},\ i\right)\supset F\left(2^{\frac{1}{3}},\sqrt{3}\right)\supset F\left(2^{\frac{1}{3}}\right)\supset F$$

易见 $(E_2:F(2^{\frac{1}{3}},\sqrt{3}))=2$。但 $\sqrt{3}\in F(2^{\frac{1}{3}})$。否则

$$F(2^{\frac{1}{3}})\supset F(\sqrt{3})\supset F$$

而 $(F(2^{\frac{1}{3}}):F)=3$，$(F(\sqrt{3}):F)=2$，与定理 1 矛盾．这样

$$(F(2^{\frac{1}{3}},\sqrt{3}):F(2^{\frac{1}{3}})=2 \qquad (E_2:F(2^{\frac{1}{3}}))=4$$

于是由 $(F(2^{\frac{1}{3}}):F)=3$ 得 $(E_2:F)=12$。

§4. 多项式的分裂域

1. 证明，有理数域F上多项式 x^4+1 的分裂域是一个单扩域$F(\alpha)$，其中 α 是 x^4+1 的一个根。

解 在复数域C里

$$x^4+1=(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$$

所以在C里 x^4+1 的 4 个根是

$$\alpha_1=\frac{\sqrt{2}}{2}(1+i),\ \alpha_2=\frac{\sqrt{2}}{2}(1-i),$$

$$\alpha_3=-\alpha_1,\ \alpha_4=-\alpha_2$$

由于 $\alpha_2=-\alpha_1^3$，得$F(\alpha_1,\alpha_2,\alpha_3,\alpha_4)=F(\alpha_1)$，所以单扩域$F(\alpha_1)$ 就是 x^4+1 在F上的分裂域。

2. 令F是有理数域，x^3-a 是F上一个不可约多项式而 α 是 x^3-a 的一个根。证明，$F(\alpha)$ 不是 x^3-a 在F上的分裂域。

解 x^3-a的三个根是$a^{\frac{1}{3}}$，$a^{\frac{1}{3}}\omega$，$a^{\frac{1}{3}}\omega^2$，其中

$$\omega=\frac{-1+\sqrt{3}i}{2} \qquad \omega^3=1$$

x^3-a在F上的分裂域是

$$E=F(a^{\frac{1}{3}},\ a^{\frac{1}{3}}\omega,\ a^{\frac{1}{3}}\omega^2)=F(a^{\frac{1}{3}},\ \omega)$$

我们有$F(a^{\frac{1}{3}},\ \omega)\supset F(a^{\frac{1}{3}})\supset F$. 由于$\omega$不属于$F(a^{\frac{1}{3}})$而$\omega$是$F(a^{\frac{1}{3}})$上多项式$x^2+x+1$的根，所以

$$(F(a^{\frac{1}{3}},\ \omega):F(a^{\frac{1}{3}}))=2$$

又由于$a^{\frac{1}{3}}$是F上不可约多项式x^3-a的根，所以

$$(F(a^{\frac{1}{3}}):F)=3$$

因此$(E:F)=6$。令α是多项式x^3-a的任一根。那么$(F(\alpha):F)=3$。所以$E\neq F(\alpha)$，即$F(\alpha)$不是x^3-a在F上的分裂域。

3. 令$p_1(x)$，$p_2(x)$，…，$p_m(x)$是域F上m个最高系数为1的不可约多项式. 证明，存在F的一个有限扩域

$$F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m)$$

其中α_i在F上的极小多项式是$p_i(x)$。

解 令$f(x)=p_1(x)p_2(x)\cdots p_m(x)$。做$f(x)$在域$F$上的分裂域$E$。$E$含有$f(x)$的所有根，因而含有$\alpha_1$，$\alpha_2$，…，$\alpha_m$，其中$\alpha_i$各是$p_i(x)$的一个根，$i=1,2,\cdots m$。因此

$$E\supset F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m)$$

由于 $p_1(x)\cdots$，$p_m(x)$ 都是 F 上最高系数为1的不可约多项式，所以它们分别是 α_1，α_2，…，α_m 在 F 上的极小多项式。由于 α_1，α_2，…，α_m 都是 F 上的代数元，所以 $F(\alpha_1, \alpha_2, \cdots, \alpha_m)$ 是 F 上的一个有限扩域。

4．令 P 是一个特征为素数 p 的域，$F=P(\alpha)$ 是 P 的一个单扩域，而 α 是 $P[x]$ 的多项式 x^p-a 的一个根。$P(\alpha)$ 是不是 x^p-a 在 P 上的分裂域？

解 由于 α 是 x^p-a 的一个根，所以 $\alpha^p=a$。但域 P 因而域 F 的特征是 p，所以在 $F[x]$ 中

$$x^p-a=x^p-\alpha^p=(x-\alpha)^p$$

这样 $P(\alpha)$ 是添加 x^p-a 的 p 个相同的根于 P 而得到的，因此 $P(\alpha)$ 是 x^p-a 在 P 上的分裂域。

§5. 有限域

1．令 F 是一个含 p^n 个元的有限域。证明，对于 n 的每一个因数 $m>0$，存在并且只存在 F 的一个有 p^m 个元的子域 L。

解 令 F 所含素域为 Δ，那么根据本节定理2，F 是多项式 $x^{p^n}-x$ 在 Δ 上的分裂域，若正整数 m 整除 n：$n=md$，那么 $p^n-1=(p^m)^d-1$，因而 $p^m-1\mid p^n-1$：$p^n-1=(p^m-1)t$。于是

$$x^{p^n}-x=x(x^{p^n-1}-1)=x[(x^{p^m-1})^t-1]$$

由此得 $x^{p^m-1}-1\mid x^{p^n-1}-1$，即 $x^{p^m}-x\mid x^{p^n}-x$。但 F 含 $x^{p^n}-x$ 的所有根，因此 F 也含 $x^{p^m}-x$ 的所有根。由定理3的证

明，这些根作成一个有 p^m 个元的F的子域L。若 L_1 也是一个有 p^m 个元的F的子域，那么根据定理 2，L_1 也是由 $x^{p^m}-x$ 在F中的所有根作成的，因而 $L_1=L$。

2. 一个有限域一定有比它大的代数扩域。

解 令F是一个含有 p^n 个元的有限域。在F上做多项式 $x^{p^{2n}}-x$ 的分裂域E，那么$F\subset E$，并且E是F的一个代数扩域。但E至少含有多项式 $x^{p^{2n}}-x$ 的 p^{2n} 个不同的根，因此E大于F。

读者可以自己证明，E 实际上是 $x^{p^{2n}}-x$ 在F所含素域Δ上的分裂域。

3. 令F是一个有限域，Δ是它所含素域并且 $F=\Delta(\alpha)$。α是否必须是F的非零元所作成的乘群的一个生成元？

解 令Δ是特征为 3 的素域，它的元用0，1，2来表示。这三个元都不是 $f(x)=x^2+1$ 的根，所以 $f(x)$ 是Δ上的一个不可约多项式。做Δ上单代数扩域 $F=\Delta(\alpha)$，其中α在Δ上的极小多项式是 $f(x)$。那么F有 9 个元而F的非零元所作成的乘群F^*的阶是 8。但

$$\alpha^2=-1 \qquad \alpha^4=1$$

所以α不是F^*的一个生成元。

4. 令Δ是特征为 2 的素域。找出$\Delta[x]$的一切三次不可约多项式。

解 因为Δ只有两个元 0 和 1，而$\Delta[x]$的常数项为 0 的三次多项式显然可约，所以$\Delta[x]$最多有以下 4 个三次不可约的多项式：

x^3+x^2+x+1，x^3+x^2+1，x^3+x+1，x^3+1

但1是 x^3+x^2+x+1 和 x^3+1 的根，所以这两个多项式在 Δ 上可约。因为0和1都不是 x^3+x^2+1 和 x^3+x+1 的根，所以只有后两个多项式是 $\Delta[x]$ 的不可约多项式。

§6. 可离扩域

1. 令域 F 的特征是 p，$f(x)$ 是 F 上一个不可约多项式，并且 $f(x)$ 可以写成 F 上 x^{p^e} 但不能写成 $x^{p^{e+1}}$ 的多项式 $(e\geqslant 1)$。证明，$f(x)$ 的每一个根的重复度都是 p^e。

解 设 $f(x)=g(x^{p^e})$，这里 $g(x)$ 是 F 上一个多项式。由于 $f(x)$ 在 F 上不可约，并且 $f(x)$ 不能写成 F 上 $x^{p^{e+1}}$ 的多项式，所以 $g(x)$ 在 F 上不可约并且不能写成 F 上 x^p 的多项式。因此由引理1，$g(x)$ 没有重根。令 E 是多项式 $f(x)$ $g(x)$ 在 F 上的一个分裂域、那么在 E 里

$$g(x)=a_m(x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$$

这里 $a_m\in F$，$\beta_i\in E$，$i=1, 2, \cdots, m$，并且当 $i\neq j$ 时，$\beta_i\neq\beta_j$。而

$$f(x)=g(x^{p^e})=a_m(x^{p^e}-\beta_1)(x^{p^e}-\beta_2)\cdots(x^{p^e}-\beta_m)$$

令 α 是 $f(x)$ 在 E 里的任何一个根，那么

$$(1)\qquad f(\alpha)=a_m(\alpha^{p^e}-\beta_1)(\alpha^{p^e}-\beta_2)\cdots(\alpha^{p^e}-\beta_m)=0$$

由于 β_i $(i=1, 2, \cdots, m)$ 各不相等，(1) 式中只有一个因子

$$\alpha^{p^e}-\beta_i=0,\ \text{即}\ \alpha^{p^e}=\beta_i$$

由于 $f(x)$ 在 E 中完全分解，所以在 E 中有 $f(x)$ 的 m 个

不同的根α_i，使$\alpha_i^{p^e}=\beta_i(i=1, 2, \cdots, m)$。这样

$$f(x)=a_m(x^{p^e}-\alpha_1^{p^e})(x^{p^e}-\alpha_2^{p^e})\cdots(x^{p^e}-\alpha_m^{p^e})$$

$$=a_m(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_m)^{p^e}$$

因而$f(x)$的每一个根的重复度都是p^e。

2. 设域F没有不可离扩域。证明，F的任一代数扩域都没有不可离扩域。

解 设E是F的一个代数扩域而α是E上的一个代数元。令α在E上的极小多项式是

$$f(x)=x^n+\beta_{n-1}x^{n-1}+\cdots+\beta_0$$

那么由于E是F的代数扩域，β_0，…，β_{n-1}都是F上的代数元。于是α是F上有限扩域$F(\beta_0, \cdots, \beta_{n-1})$的代数元，因而也是$F$上的代数元。但$F$没有不可离扩域，所以$\alpha$是$F$上可离元，而$\alpha$在$F$上的极小多项式$g(x)$没有重根。但$f(x)|g(x)$，所以$f(x)$也没有重根，而$\alpha$是$E$上的可离元。这样，$E$上的任意代数元都是$E$上的可离元，即$E$没有不可离扩域。

3. 令域F的特征是p而$E=F(\alpha, \beta)$，这里α是F上n次可离元，而β是F上p次非可离元。$(E:F)=$?

解 按照题设，β在F上的极小多项式$f(x)$的次数是p。令β在$F(\alpha)$上的极小多项式是$h(x)$，那么$h(x)|f(x)$，因而$h(x)$的次数$\leqslant p$。

设 $h(x)$的次数小于p。那么$h(x)$不能写成$g(x^p)$的形式，这里$g(x)$是$F(\alpha)[x]$的一个多项式。因此β是$F(\alpha)$上的一个可离元。但α是F上一个可离元，所以根据引理4，β也是F上一个可离元，与β是F上一个非可离元

的题设矛盾。这样，$h(x)$ 的次数是 p。于是有

$$(F(\alpha, \beta) : F(\alpha)) = p, \quad (F(\alpha) : F) = n,$$

$$(E : F) = (F(\alpha, \beta) : F(\alpha))(F(\alpha) : F) = pn$$

4. 找一个域 F，使 F 有一个有限扩域 E 而 E 不是 F 的单扩域。

解 令 Δ 是特征为 2 的素域，$F = \Delta(x, y)$，这里 x 和 y 是 F 上两个无关未定元。考察 $E = F(\sqrt{x}, \sqrt{y})$，这里 $\sqrt{x}$ 和 $\sqrt{y}$ 在 F 上的极小多项式各是

$$z^2 - x \text{ 和 } z^2 - y$$

由于 $\sqrt{y} \notin F(\sqrt{x})$，所以 $\sqrt{y}$ 在 $F(\sqrt{x})$ 上的极小多项式仍是 $z^2 - y$。这样

$$(E : F(\sqrt{x})) = 2, (F(\sqrt{x}) : F) = 2, (E : F) = 4$$

E 的任一元 α 都可以写成 F 上 $\sqrt{x}$ 和 $\sqrt{y}$ 的多项式：

$$\alpha = f(\sqrt{x}, \sqrt{y})$$

由于 F 的特征是 2，这样一个多项式的二次方等于它的各项的二次方的和，因而 $\alpha^2 = g(x, y)$，这里 $g(x, y)$ 是 F 上 x 和 y 的多项式。因此 $\alpha^2 \in F$。这就是说，E 的任一元 α 在 F 上的次数最多是 2。这样，F 上四次扩域 E 不可能是一个单扩域 $F(\alpha)$。